

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09023

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.<sup>7</sup> G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.<sup>7</sup> G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Jitsuyo Shinan Toroku Koho	1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JOIS (JICST)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Denshi Shotorihiki Dai 4 kai Denshi Kessai no Houhou to Kinou", bit, Vol.31, No.6, Kyouritsu Shuppan K.K., pp.99-105 (01.06.99)	1-27
Y	JP, 10-154193, A (NTT Data Tsushin K.K.), 09 June, 1998 (09.06.98), Full text; Figs. 1 to 23 (Family: none)	1-27
Y	JP, 10-049584, A (Canon Inc.), 20 February, 1998 (20.02.98), Full text; Figs. 1 to 13 & CA, 2212027, A & EP, 0823820, A2 & AU, 701005, B	1-61
Y	JP, 11-296602, A (Hitachi, Ltd.), 29 October, 1999 (29.10.99), Full text; Figs. 1 to 14 (Family: none)	28-61
Y	JP, 10-283320, A (NTT DATA CORPORATION), 23 October, 1998 (23.10.98), Full text; Figs. 1 to 13 (Family: none)	28-61

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

14 March, 2001 (14.03.01)

Date of mailing of the international search report

27 March, 2001 (27.03.01)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09023

## Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The technical feature of the inventions of claims 1-27 is an electronic money or electronic license the security of which is changeable by the issuer or manager.  
The technical feature of the inventions of claims 28-61 is to perform security check of an electronic money or electronic license and perform at least either stop of the operation of the system or notification to the effect that the result of the check shows incorrectness if the result of the security check shows incorrectness.  
These groups of inventions are not united into one invention nor so linked as to form a single general inventive concept.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
  
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
  
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
 日本国公開実用新案公報 1971-2001年  
 日本国登録実用新案公報 1994-2001年  
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JOIS (JICST)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	「電子商取引 第4回電子決済の方法と機能」, bit Vol.31 No.6, 共立出版株式会社, 第99-105頁 (01.06.99)	1-27
Y	JP, 10-154193, A (エヌ・ティ・ティ・データ通信 株式会社) 9.6月. 1998 (09.06.98) 全文, 第1-23図 (ファミリーなし)	1-27
Y	JP, 10-049584, A (キヤノン株式会社) 20.2月. 1998 (20.02.98) 全文, 第1-13図 & CA, 2212027, A & EP, 0823820, A2	1-61

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」 口頭による開示、使用、展示等に言及する文献  
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」 同一パテントファミリー文献

国際調査を完了した日

14.03.01

国際調査報告の発送日

27.03.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
 郵便番号100-8915  
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丹治 彰



5L 8320

電話番号 03-3581-1101 内線 3560

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	& AU, 701005, B	
Y	JP, 11-296602, A (株式会社日立製作所) 29. 10月. 1999 (29. 10. 99) 全文, 第1-14図 (ファミリーなし)	28-61
Y	JP, 10-283320, A (株式会社エヌ・ティ・ティ・ データ) 23. 10月. 1998 (23. 10. 98) 全文, 第1-13図 (ファミリーなし)	28-61

## 第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

請求の範囲1-27は、電子マネー、又は電子利用権であって、そのセキュリティを発行元又は管理者が変更可能とされたことを技術的特徴とするものである。

請求の範囲28-61は、電子マネー、又は電子利用権のセキュリティチェックを行い、セキュリティチェックの結果が正しくないときには、システムの稼働等の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを技術的特徴とするものである。

これらは一の発明であるとも、単一の一般的発明概念を形成するように連関している一群の発明であるとも認められない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**THIS PAGE BLANK (USPTO)**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09023

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Jitsuyo Shinan Toroku Koho	1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JOIS (JICST)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Denshi Shotorihiki Dai 4 kai Denshi Kessai no Houhou to Kinou", bit, Vol.31, No.6, Kyouritsu Shuppan K.K., pp.99-105 (01.06.99)	1-27
Y	JP, 10-154193, A (NTT Data Tsushin K.K.), 09 June, 1998 (09.06.98), Full text; Figs. 1 to 23 (Family: none)	1-27
Y	JP, 10-049584, A (Canon Inc.), 20 February, 1998 (20.02.98), Full text; Figs. 1 to 13 & CA, 2212027, A & EP, 0823820, A2 & AU, 701005, B	1-61
Y	JP, 11-296602, A (Hitachi, Ltd.), 29 October, 1999 (29.10.99), Full text; Figs. 1 to 14 (Family: none)	28-61
Y	JP, 10-283320, A (NTT DATA CORPORATION), 23 October, 1998 (23.10.98), Full text; Figs. 1 to 13 (Family: none)	28-61

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier document but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
14 March, 2001 (14.03.01)Date of mailing of the international search report  
27 March, 2001 (27.03.01)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile N .

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09023

## Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The technical feature of the inventions of claims 1-27 is an electronic money or electronic license the security of which is changeable by the issuer or manager.  
The technical feature of the inventions of claims 28-61 is to perform security check of an electronic money or electronic license and perform at least either stop of the operation of the system or notification to the effect that the result of the check shows incorrectness if the result of the security check shows incorrectness.  
These groups of inventions are not united into one invention nor so linked as to form a single general inventive concept.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
  
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
  
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JOIS (JICST)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	「電子商取引 第4回電子決済の方法と機能」, bit Vol.31 No.6, 共立出版株式会社, 第99-105頁 (01.06.99)	1-27
Y	JP, 10-154193, A (エヌ・ティ・ティ・データ通信 株式会社) 9.6月.1998 (09.06.98) 全文, 第1-23図 (ファミリーなし)	1-27
Y	JP, 10-049584, A (キヤノン株式会社) 20.2月.1998 (20.02.98) 全文, 第1-13図 & CA, 2212027, A & EP, 0823820, A2	1-61

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

14.03.01

国際調査報告の発送日

27.03.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丹治 彰



5L

8320

電話番号 03-3581-1101 内線 3560

## C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	& AU, 701005, B	
Y	JP, 11-296602, A (株式会社日立製作所) 29. 10月. 1999 (29. 10. 99) 全文, 第1-14図 (ファミリーなし)	28-61
Y	JP, 10-283320, A (株式会社エヌ・ティ・ティ・ データ) 23. 10月. 1998 (23. 10. 98) 全文, 第1-13図 (ファミリーなし)	28-61

## 第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-27は、電子マネー、又は電子利用権であって、そのセキュリティを発行元又は管理者が変更可能とされたことを技術的特徴とするものである。

請求の範囲28-61は、電子マネー、又は電子利用権のセキュリティチェックを行い、セキュリティチェックの結果が正しくないときには、システムの稼働等の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを技術的特徴とするものである。

これらは一の発明であるとも、単一の一般的発明概念を形成するように連関している一群の発明であるとも認められない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。  
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**THIS PAGE BLANK (USPTO)**

## 明 細 書

## 電子マネーシステム

- 5      この発明は、電子マネー、電子利用権、課金システムおよび情報処理装置、コンテンツデータの再生方法並びに再生制御方法に関する。特にこの発明は、セキュリティのかけられた電子マネー、電子利用権、並びにこれらのいずれかを用いる課金システム、情報処理装置、コンテンツデータの再生方法、再生制御方法に関する。

## 10   背景技術

- 現金と同様に流通する電子マネーが実用化されようとしている。電子マネーは、ＩＣカードに蓄積する。電子マネーとしては、プリペイド型、後払い型がある。さらに、インターネットとパーソナルコンピュータ（パソコン）とを使用して、自分の金融機関の口座からＩＣカードに入金したり、未使用分を口座に入金することも提案されている。電話使用料、乗車券等の電子利用権をＩＣカード、特に、非接触型のＩＣカードを介して実現する試みもなされている。

- これらの電子マネー、電子利用権は、情報をＩＣカードに蓄積するので、既存の磁気ストライプ型のカードに比して、偽造が難しい利点がある。セキュリティ対策として、リーダ・ライタとＩＣカードと間でやり取りされるデータが暗号化されることが考えられている。

- しかしながら、たとえリーダ・ライタとＩＣカードの間でやりとりされるデータの暗号化を行っていても、電子マネー、電子利用権のセキュリティが充分であるとは言えない。電子マネー、電子利用権を配信された音楽等のデジタルコンテンツを利用するための対価として使用することが考えられる。デジタルコンテンツ自身に対しては、

強力な暗号化や、コピープロテクション等の処理が施されているのと比較して、電子マネー、電子利用権のセキュリティが高くはなかった。デジタルコンテンツの利用と、電子マネー、電子利用権との共同作業がないことも、セキュリティの面で弱い原因となっていた。ディ

5 ジタルコンテンツは、電子マネー、電子利用権とは異なり、一旦流通すると、一元管理が難しく、コンテンツに対する暗号が破られたような場合に、再び別な暗号化処理を行う等の必要性が生じるためシステムの変更に多大な労力を要する。

したがって、この発明の目的は、このような点に鑑み、よりセキュ

10 リティを向上することができる電子マネー、電子利用権、課金システムおよび情報処理装置、コンテンツデータの再生方法並びに再生制御方法を提供することにある。

#### 発明の開示

上述した課題を解決するために、請求の範囲 1 の発明は、現金に相

15 当する効力を有する電子マネーであって、

そのセキュリティを発行元または管理者が変更可能とされたことを特徴とする電子マネーである。

請求の範囲 6 の発明は、コンテンツの再生等のソフトウェアの利用を可能とする電子利用権であって、

20 そのセキュリティを発行元または管理者が変更可能とされたことを特徴とする電子利用権である。

請求の範囲 1 2 の発明は、圧縮符号化および／または暗号化されたソフトウェアが配布され、配布されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子マネーを介して課金処理がなされる

25 ようにした課金システムであって、

電子マネーのセキュリティを発行元または管理者が変更可能とされ

たことを特徴とする課金システムである。

請求の範囲 20 の発明は、圧縮符号化および／または暗号化されたソフトウェアが配布され、配布されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子利用権を介して課金処理がなされる

5 ようにした課金システムであって、

電子利用権のセキュリティを発行元または管理者が変更可能とされたことを特徴とする課金システムである。

請求の範囲 28 の発明は、電子マネーまたは電子利用権を用いることによって稼働しているシステムであって、

10 電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システムである。

請求の範囲 33 の発明は、圧縮符号化および／または暗号化されたソフトウェアが配布され、配布されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子マネーまたは電子利用権を介して課金処理がなされるようにした課金システムであって、

電子マネーまたは電子利用権のセキュリティチェックを行い、

20 セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システムである。

請求の範囲 38 の発明は、配布された圧縮符号化および／または暗号化されたソフトウェアを復号するに際し、電子マネーまたは電子利用権を介して課金処理がなされるようにした情報処理装置であって、

25 電子マネーまたは電子利用権のセキュリティチェックを行い、

セキュリティチェックの結果が正しくないときには、ソフトウェア

の復号の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする情報処理装置である。

請求の範囲 4 3 の発明は、圧縮および／または暗号化されたコンテンツデータを再生処理する際に電子利用権のセキュリティをチェックし、

セキュリティチェックの結果、電子利用権が有効でない場合にはコンテンツデータの再生を中止し、

セキュリティチェックの結果、電子利用権が有効であった場合には  
10 コンテンツデータの再生処理を行うとともに電子利用権を消費するコンテンツデータの再生方法である。

請求の範囲 4 9 の発明は、圧縮および／または暗号化されたコンテンツデータを再生処理にあたって行われる課金処理に用いられる電子利用権のセキュリティをチェックし、

15 セキュリティチェックの結果、電子利用権が有効でない場合にはコンテンツデータの再生を中止し、

セキュリティチェックの結果、電子利用権が有効であった場合にはコンテンツデータの再生処理を行うとともに電子利用権に基づき課金処理を行うコンテンツデータの再生方法である。

20 請求の範囲 5 7 の発明は、管理機構から購入した電子利用権をプレーヤ内のメモリに記憶し、

プレーヤによって圧縮および／または暗号化されたコンテンツデータを再生処理にあたって行われる課金処理に用いられる電子利用権のセキュリティをチェックし、

25 セキュリティチェックの結果、電子利用権が有効でない場合にはコンテンツデータの再生を中止し、

セキュリティチェックの結果、電子利用権が有効であった場合にはコンテンツデータの再生処理を行うとともに電子利用権に基づき課金処理を行う再生制御方法である。

#### 図面の簡単な説明

- 5 第1図は、この発明の一実施形態のシステム全体の概略を示すブロック図である。

第2図は、この発明の一実施形態における聴取権データに関する説明のためのブロック図である。

- 10 第3図は、この発明の一実施形態における聴取権データチャージャに関する説明のためのブロック図である。

第4図は、この発明の一実施形態における聴取権データに関する説明のためのブロック図である。

第5図は、この発明の一実施形態における決済センターの果たす機能に関する説明のためのブロック図である。

- 15 第6図は、この発明の一実施形態におけるプレーヤの一例のブロック図である。

第7図は、この発明の一実施形態における課金処理の一例を説明するためのフローチャートである。

- 20 第8図は、この発明の一実施形態における聴取権データチャージャの一例のブロック図である。

第9図は、この発明の一実施形態におけるセキュアデコーダのより詳細なブロック図である。

第10図Aおよび第10図Bは、この発明の一実施形態における聴取権データのデータ構成の一例の略線図である。

- 25 第11図は、この発明の一実施形態における聴取権データのセキュリティチェックとコンテンツ再生との関連する処理を説明するための

フローチャートである。

発明を実施するための最良の形態

以下、この発明を音楽配信システム EMD (Electronic Music Distribution) に適用した一実施形態について説明する。最初に第 1 図を  
5 参照して音楽配信システムの概略について説明する。第 1 図において、指示符号 101 が音楽コンテンツ供給事業者例えばレコード会社を示し、指示符号 102 がコンテンツサーバを示す。レコード会社 101 が音楽コンテンツの制作およびその配給を行う。音楽コンテンツに関するの圧縮符号化、暗号化、ウォーターマークの埋め込みもレコード会社 101 が行う。コンテンツサーバ 102 には、レコード会社 101 が制作した音楽コンテンツをはじめとするコンテンツデータが蓄積される。  
10

指示符号 103 は、著作権管理機構を示す。例えば JASRAC (日本音楽著作権協会) は、著作権管理機構 102 の具体例である。レコード会社 101 は、著作権管理機構 103 に対して音楽コンテンツの著作権に関する権利登録を行い、著作権管理機構 103 から著作権料を受け取る。  
15

指示符号 104 が配信された音楽コンテンツの再生機能を有するユーザデバイスを示す。ユーザデバイス 104 は、配信された音楽コンテンツとしてのコンテンツデータを再生すると共に、再生課金の処理を行う機能を有する。すなわち、配信された音楽コンテンツとしてのコンテンツデータに施されている暗号を復号し、圧縮符号化を復号することによって、コンテンツデータを再生することができ、コンテンツデータの復号に対し、すなわち音楽コンテンツの再生により課金  
20 される。コンテンツサーバ 102 とユーザデバイス 104 との間には、必要に応じてコンテンツ配信事業者が介在し、ユーザに対してコン  
25

テンツサーバ 102 内のコンテンツデータを配信する。配信事業者が使用する配信手段としては、幾つかのものがある。その一つは、販売店 105 である。例えば雑誌の付録として、コンテンツが記録されたメディア、例えば CD-ROM、CD 等のディスク等の媒体が配付される。また、インターネット、CATV (cable television) のような有線ネットワーク 106 がコンテンツの配信手段として使用される。さらに、携帯電話網 107、衛星放送、衛星通信等の衛星ネットワーク 108 もコンテンツの配信手段として用いることができる。

この発明では、上述したコンテンツ配信手段として、有料で配信されるコンテンツの配信手段を利用することを妨げるものではない。媒体例えば CD (Compact Disc; CD、登録商標) の場合には、記録されている楽曲に対しての著作権料が CD の価格に含まれている。配付を無料とし、復号 (再生) に課金されるコンテンツデータを CD 上の有料コンテンツデータが記録された記録領域とは別の記録領域に記録するようにしても良い。

第 1 図中では、販売店 105 が配付する媒体の一つとしての拡張 CD 121 が示されている。拡張 CD 121 の内周側の記録領域 122 は、既存の CD と同一のフォーマットで、配付が有料で、再生が無料とされたコンテンツデータとしての楽曲データが記録された領域である。内周側の記録領域 122 の外周側に設けられている外周側の記録領域 123 は、配付が無料で、再生が有料のコンテンツデータが記録された領域である。記録領域 123 に記録されるコンテンツデータには、圧縮符号化処理が施されているので、領域 123 には少なくとも必要な長さの音楽データ、例えば伸張処理を行った状態で内周側の記録領域 122 に記録されているコンテンツデータと同等の長さを有するコンテンツデータを記録することができる。

CD 以外に MD (Mini Disc ; 登録商標)、メモリカード等の媒体の場合にも、互いに区別できる領域として、配付が有料で、且つ再生が無料のコンテンツデータと、配付が無料で、且つ再生が有料のコンテンツデータとを記録することができる。衛星テレビジョン放送を利用して音楽コンテンツを配信するサービスを利用して配付が無料で、再生が有料のコンテンツデータを配信しても良い。

ユーザデバイス 104 は、配信されてくるまたは配布されたコンテンツデータを無料で受け取ることができる。ユーザは受け取ったコンテンツデータを通信回線網を介して他の人に再配付も自由に行うことができる。ここで、「無料」というのは、通信費、電気代等の実費を含まず、著作権料に関して無料という意味である。ユーザデバイス 104 が受け取ったコンテンツデータを再生、より具体的には、コンテンツデータに施されている暗号化を復号する時に著作権料を含む課金処理が行われる。この課金処理のために、聴取権データ 109 が使用される。聴取権データ 109 は、IC カード、セキュアデコーダ内のメモリに格納されている。聴取権データ 109 は、聴取権データ管理会社の管理下で、ユーザが所有する課金チャージャまたは最寄りの販売店に設置された販売端末によって書き換えることが可能とされている。聴取権データ 109 は、例えば音楽コンテンツ等のコンテンツとしてのコンテンツデータの再生可能な度数であり、ユーザデバイス 104 が課金の対象のコンテンツを再生する度に、聴取権データ 109 としての度数が減算される。

以下の説明では、電子利用権としての聴取権データ 109 を例に説明するが、後述する聴取権データの構成をそのまま踏襲した電子マネーをコンテンツデータの再生の支払いに当てることもできる。さらに、電子マネー、聴取権データ等を一括して扱うことができる多目的 I

Cカードを使用することもできる。

レコード会社101、著作権管理機構103、ユーザデバイス104と関係して代金決済のために、決済センター110が存在している。決済センター110は、認証／課金サーバ111を備えている。決済センター110は、銀行、クレジットカード会社208との間で、代金の決済を行う。

ユーザデバイス104が配信または配布されたコンテンツデータの再生を要求すると、認証／課金サーバ111に対してユーザデバイス104の認証を要求する（A1の経路で示す）。ユーザID等に基づいてユーザデバイス104が正規のものであり、認証が成立すると、認証／課金サーバ111は、ユーザデバイス104に対してコンテンツデータ再生のための課金の要求を行う（経路A2）。ユーザデバイス104は、決済センター110との間で、代金決済を行う（経路A3）。

決済センター110は、認証／課金サーバ111に対して、経路A4で示すように、課金がされたことまたは課金処理が可能であることを伝達すると共に、コンテンツサーバ102に対してコンテンツデータの送信を要求する（経路A5）。コンテンツサーバ102が認証／課金サーバ111にコンテンツデータに施されている暗号を復号するための鍵データを渡す（経路A6）。認証／課金サーバ111がユーザデバイス104に対して、コンテンツサーバ102から渡された鍵データを渡す（経路A7）。ユーザデバイス104は、サーバ111から送信されてきた鍵データによって、コンテンツデータに施されている暗号を復号化し、コンテンツデータを再生することができる。コンテンツデータが復号されることをもって、そのコンテンツの再生がされたものと判断され、聴取権データ109の度数が例えば「-1」

される。聴取権データ 109 の度数が「0」に達すると、ユーザデバイス 109 がコンテンツデータの復号ができなくなる。

第 2 図は、聴取権データ 109 に関するシステムの一例を示し、音楽コンテンツの配信、音楽コンテンツとしてのコンテンツデータの暗号の復号をするためのデータの授受については、省略されている。ユーザデバイス 104 に対応するものとして、プレーヤ 201 が示されている。プレーヤ 201 は、セキュアデコーダ 202 を内蔵している。プレーヤ 201 は、例えば携帯形オーディオ記録および／または再生機器である。第 2 図において、破線で示すように、プレーヤ 201 が再生する媒体（光ディスク、メモリカード等）には、音楽コンテンツが記録、記憶されている。音楽コンテンツの配信、配布の方法は、第 1 図に示したように、種々のものを使用できる。

指示符号 204 は、ユーザ端末としての聴取権データチャージャを示す。データチャージャ 204 は、プレーヤ 201 のセキュアデコーダ 202 と決済センター 110 またはレコード店、コンビニエンスストア等に設置されているデータ販売端末 206 との間に存在して聴取権データ中継器として機能する。

第 3 図は、データチャージャ 204 の機能を概略的に示すものである。第 3 図において、家庭内に設置される可能性のあるプレーヤ 201 の具体例が示されている。指示符号 51 がアンプとスピーカとが別体とされたオーディオ再生装置であり、指示符号 52 がチューナ、CD プレーヤ（または MD レコーダ）が一体化された再生機器であり、指示符号 53 が携帯型 CD プレーヤであり、指示符号 54 が携帯型 MD プレーヤであり、指示符号 55 がパーソナルコンピュータである。これらのユーザデバイスには、IC 構成のセキュアデコーダ 51a、52a、53a、54a、55a が装備されている。これらのユーザ

デバイスに対して、データチャージャ 204 が共用され、専用接続線あるいは非接触無線通信、または USB (Universal Serial Bus) あるいは IEEE (Institute of Electrical and Electronics Engineers) 1394 によって、聴取権データの送信と、再生履歴情報の吸い上げを行うことができる。データチャージャ 204 は、携帯可能な構成とされている。

プレーヤ 201 内のセキュアデコーダ 202 とデータチャージャ 204 とが有線または無線の通信路を介して通信を行い、聴取権データ 109 がデータチャージャ 204 からセキュアデコーダ 202 内のメモリに対して転送される。聴取権データ 109 は、例えばプレーヤ 201 の再生可能回数情報または再生可能時間に対応している。

プレーヤ 201 からデータチャージャ 204 に対して、有線または無線の通信路 205 を介してプレーヤ 201 の再生履歴情報（再生ログ）が伝送される。再生ログは、復号したデジタルデータの識別子および／または復号の条件を含む。具体的には、聴取した音楽コンテンツの種類、再生回数、再生時間等の情報を含んでいる。再生ログには、ユーザ端末の所有者、ユーザデバイスの識別子等の課金対象者を特定するための識別子が含まれている。セキュアデコーダ 202 とデータチャージャ 204 とは、必要に応じて認証を行い、認証が成立すると、暗号化された聴取権データおよび再生ログの伝送がなされる。

聴取権データ 109 は、決済センター 110 から通信路 207 例えば電話回線を介してデータチャージャ 204 に渡される。または、決済センター 110 から通信路 209 を介して販売端末 206 に渡された聴取権データ 109 が通信路 205 を介してデータチャージャ 204 に渡される。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。

データチャージャ 204 に吸い上げられた再生ログは、通信路 207 を介して決済センター 110 に送られる。または、通信路 205 を介して販売端末 206 に渡される。販売端末 206 は、通信路 209 を介して決済センター 110 から聴取権データ 109 を受け取ると共に、再生ログを決済センター 110 へ送る。さらに、入手した聴取権データの代金を決済センター 110 に支払う。通信路 209 は、電話回線、インターネット等である。

決済センター 110 と聴取権データチャージャ 204 との間では、通信路 207 を介して聴取権データ 109 および再生ログの送受信がなされる。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。聴取権データ 109 の決済に関して、銀行、クレジットカード会社 208 が存在している。銀行、クレジットカード会社 208 は、予め登録してあるユーザの銀行口座から決済センター 110 の依頼に基づいて、データチャージャ 204 に書き込んだ聴取権データに相当する金額を引き落とす。

さらに、決済センター 110 は、レコード会社 101 から聴取権データ 109 に関するサービスの管理の委託を受ける。また、決済センター 110 は、レコード会社 101 に対して聴取権データ 109 に関する技術の提供を行い、さらに、楽曲聴取料を支払う。レコード会社 101 は、第 1 図を参照して説明したように、著作権管理機構 103 に対して著作権の登録を行うことによって、著作権の管理を依頼し、著作権管理機構 103 から著作権料を受け取る。

第 2 図では省略しているが、聴取権データチャージャ 204 は、他のチャージャとの間で、通信装置例えば非接触通信装置を通じて、聴取権データの一部または全部を移動・合算・分割可能とされている。データチャージャ 204 は、プレーヤ 201 のセキュアデコーダ 20

2 以外に I C カードの構成のプリペイドカードに対して聴取権データ  
1 0 9 を転送可能とされている。

第 4 図は、第 2 図に示される課金処理システムにおけるレコード会  
社 1 0 1、決済センター 1 1 0、聴取権データチャージャ 2 0 4、聴  
5 取権データ販売端末 2 0 6 および銀行、クレジットカード会社 2 0 8  
の相互の関係を抜き出したものである。決済センター 1 1 0 がチャ  
ージャ 2 0 4 および販売端末 2 0 6 との間で、聴取権データ 1 0 9 の販  
売を行い、また、再生ログを収拾し、聴取権データに基づいて代金の  
決済を行う機能を有する。

10 第 5 図は、聴取権データ端末 2 1 0（聴取権データチャージャ 2 0  
4 または販売端末 2 0 6）と接続された決済センター 1 1 0 の機能を  
より詳細に示すものである。第 5 図中で、実線の経路は、課金処理を  
実行する上で必要な処理を意味し、破線経路が課金処理を行う準備と  
して必要な処理を意味する。多くの場合、破線の経路が郵送（文書の  
15 授受）により行われ、実線の経路の処理がデータ通信を用いて行われ  
る。

最初に破線経路による処理について説明する。レコード会社 1 0 1  
と決済センター 1 1 0 の間では、レコード会社 1 0 1 が決済センター  
1 1 0 に対して業務委託登録を行う（ブロック 2 1 1）。決済セン  
20 ー 1 1 0 は、レコード会社 1 1 0 に対してマーケティングデータを渡  
したり、各種報告を行う（ブロック 2 1 2）。

聴取権データチャージャ 2 0 4 の所有者である顧客 2 1 3 は、銀行  
、クレジットカード会社 2 0 8 との間で、料金の支払い、口座からの  
料金の引き落とし等の契約を結ぶ。顧客 2 1 3 が契約内容の変更等を  
25 決済センター 1 1 0 に連絡し、決済センター 1 1 0 が顧客情報の入力  
・修正を行う（ブロック 2 1 4）。決済センター 1 1 0 が顧客 2 1 3

に対して請求書、領収書の発行とその郵送を行う（ブロック 2 1 5）

。

次に実線経路による処理について説明する。決済センター 1 1 0 が顧客の要求に応じて聴取権データ端末 2 1 0 に対して聴取権データ 1 0 9 を送る。その場合、顧客の特定がなされ、また、通信サーバ 2 1 6 を介して認証・暗号化の処理がされたデータを送る。顧客管理システム 2 1 7 は、データベース 2 1 8 中の顧客情報を参照して、認証した顧客を特定する。転送した聴取権データ 1 0 9 の量に基づいて、金融決済システム 2 1 9 に対して、顧客の銀行口座から料金の引き落としを依頼する。金融決済システム 2 1 9 が銀行、クレジットカード会社 2 0 8 に対して顧客の口座から料金の支払いを依頼し、料金の支払いが実行される。金融決算システム 2 1 9 から支払いの完了の報告を決済センター 1 1 0 が受け取ると、顧客への領収書の発行が行われる。

15 聴取権データ端末 2 1 0 に対して、決済センター 1 1 0 が聴取権データ 1 0 9 を転送するのに先行して聴取権データ端末 2 1 0 の認証が行われる。聴取権データ端末 2 1 0 から通信サーバ 2 1 6 を介して再生ログを決済センター 1 1 0 を送信する。送信されてきた再生ログが通信サーバ 2 1 6 にて暗号化が復号され、再生ログ管理システム 2 2 0 へ送られる。再生ログには、顧客（聴取権データ端末 2 1 0）を特定するための端末識別子と、復号・再生した音楽コンテンツを特定する識別子と、各音楽コンテンツを聴取した回数、時間、期間のデータとが含まれている。端末識別子は、主として上述したような聴取権データ 1 0 9 を転送する際のデータ端末 2 1 0 の認証を行う等に用いられ  
25 たり、聴取権データ 1 0 9 に対応する課金のために使用される。

再生ログ管理システム 2 2 0 が再生ログを一旦データベース 2 1 8

に格納し、予め決められた時、例えば1カ月毎にバッチ処理で再生ログまたは再生ログを処理したデータを聴取料決済システム221に渡す。聴取料決済システム221は、レコード会社101から業務委託時にデータベース218に登録した曲等の情報を参照して、曲毎の聴  
5 取料（著作権使用料）を算出する。曲以外に作曲家、作詞家、歌手、演奏者等の項目毎に聴取料を算出することも可能である。聴取料決済システム221が算出した曲毎の聴取料がレコード会社101に対して支払われる。

上述したように、決済センター110が顧客213への聴取権データ109の転送と、聴取料の請求を行い、一方、決済センター110  
10 が曲毎の聴取料を算出し、分配する処理を行うので、レコード会社101が顧客管理を行ったり、聴取料を算出したり、分配する業務を行う必要がない。決済センター110は、レコード会社101と独立した機関であるので、複数のレコード会社との間で業務委託の契約を行う  
15 うことができ、顧客が選択できる音楽コンテンツの種類を豊富にすることができ。

第6図は、セキュアデコーダ202を有するプレーヤ201の信号処理の構成を示す。セキュアデコーダ202は、破線で示すように、  
1チップのICとして構成されたものである。セキュアデコーダ20  
20 2は、所謂タンパーレジスタント(tamper resistant)の構成とされている。すなわち、外部からは、セキュアデコーダ202の内容が分からないような構成とされ、セキュアデコーダ202の改ざんができない構成とされている。

媒体1には、圧縮符号化され、また、暗号化された音楽データが記  
25 録されている。さらに、再生課金処理に必要なデータ、この場合は音楽データが圧縮符号化、暗号化されたデータに付随している。以降、

圧縮符号化、暗号化されたデータをコンテンツデータと称し、再生課金処理のためのデータを付随データと称する。但し、この発明では、圧縮符号化と暗号化との両方が施されていることは、必ずしも必要ではない。圧縮符号化のみでも、その復号方法が非公開であれば、著作権保護の目的を果たすことが可能である。

媒体 1 としては、メモ리카ード、記録可能な光ディスク、読み出し専用の光ディスク等を使用できる。記録可能な媒体の場合では、上述したように、衛星ネットワーク、携帯電話ネットワーク、インターネット等のネットワークを介して配信されたデータをダウンロードすることができる。媒体 1 に記録されているコンテンツデータおよび付随データがインターフェース 2 を介してセキュアデコーダ 202 に供給される。セキュアデコーダ 202 からは、コンテンツデータに基づくアナログオーディオ信号が出力される。セキュアデコーダ 202 から出力されるアナログオーディオ信号は、アンプ等を介してスピーカ、ヘッドフォン等によって再生される。

セキュアデコーダ 202 は、暗号化の復号器 11 と、圧縮符号化の伸張器 12 と、D/A 変換器 13 とを有している。コンテンツデータに施される暗号化としては、DES (Data Encryption Standard) を使用できる。DES は、平文をブロック化し、ブロック毎に暗号変換を行うブロック暗号の一つである。DES は、64 ビットの入力に対して 64 ビット (56 ビットの鍵と 8 ビットのパリティ) のキーを用いて暗号変換を行い、64 ビットを出力する。勿論、DES 以外の暗号化を使用しても良い。例えば DES は、暗号化と復号化に同一の鍵データを使う共通鍵方式であるが、暗号化と復号化に異なる鍵データを使う公開鍵暗号の一例である RSA 暗号を採用しても良い。鍵データは、上述したように、例えばサーバ 111 との間で認証が成立したユ

ーザデバイス 104 に対して渡される。

セキュアデコーダ 202 には、CPU を含む制御部 14 と、制御部 14 と外部の CPU との通信を行うための CPU インターフェース 15 と、メモリ部 16 と、聴取権データをプリペイドチャージャから受信し、再生ログをプリペイドチャージャに伝送するための通信部 17 およびアンテナ 18 とが設けられている。制御部 14 は、復号器 11 における復号の前段で分離された付随データを受け取り、復号化、伸張化を行うための制御を行う。通信部 17 およびアンテナ 18 は、非接触で聴取権データチャージャ 204 との間で通信を行うためのものである。この通信は、セキュアデコーダ 202 とチャージャ 204 との間で認証がされることを条件として、暗号化されたプロトコルを用いて行われる。データのみならず、電力をチャージャ 204 から供給を受けることができるので、プレーヤ 201 全体の電源がオフであっても、セキュアデコーダ 202 は聴取権データ 109 の受信と、チャージャ 204 に対して再生ログの送信とを行うことができる。チャージャ 204 から受け取った聴取権データ 109 は、メモリ部 16 に格納される。さらに、プレーヤ 201 で行われるコンテンツデータの再生によって生じる再生ログもメモリ部 16 に記憶される。メモリ部 16 は、電源オフとされても、その記憶内容が保持される不揮発性メモリである。

なお、コンテンツデータ等のコピー出力が復号器 11 からセキュアデコーダ 202 の外部に出力することが可能とされている。コンテンツデータ等のコピーを出力するか否かは、制御部 14 により制御される。出力されるコピー出力は、付随データとコンテンツデータである。さらに、復号器 11 および伸張器 12 は、制御部 14 からの制御信号、制御コマンドに基づいて、復号処理および伸張処理をそれぞれ省

略する機能を有している。それによって、例えば媒体 1 から読み出されたコンテンツデータが元々暗号化および圧縮符号化がされていないオーディオデータ、リニア P C M 信号である場合にも再生することができる。

- 5 プレーヤ 2 0 1 の全体の動作を制御するために、指示符号 2 1 で示すシステムコントローラが備えられている。システムコントローラ 2 1 は、C P U で構成され、セキュアデコーダ 2 0 2 内の制御部 1 4 と通信を行うことによって、セキュアデコーダ 2 0 2 の動作を制御する。システムコントローラ 2 1 とバスを介して操作部 2 2、ディスプレイ 10 イ 2 3、メモリ部 2 4、モデム 2 5 が接続されている。さらに、システムコントローラ 2 1 が例えば操作部 2 2 からの操作入力に基づいて媒体 1 の再生動作、並びに媒体インターフェース 2 の動作を制御する。

- 操作部 2 2 は、ユーザが操作する複数のスイッチ、複数のキー等から構成されており、プレーヤ 2 0 1 の動作を制御する制御信号を発生する。ディスプレイ 2 3 は、例えば液晶表示素子から構成されており、例えばユーザが操作部 2 2 を用いてプレーヤ 2 0 1 の動作を制御するためのメニューを表示したり、プレーヤ 2 0 1 の動作状態を表示する。メモリ部 2 4 は、システムコントローラ 2 1 内のメモリの容量が 20 少ないために設けられた外部メモリである。モデム 2 5 は、公衆回線と接続され、外部とのまたは外部の機器とデータの通信に使用される。例えば、セキュアデコーダ 2 0 2 のメモリ部 1 6 内の再生ログをメモリ部 2 4 に転送することによって、残りの再生可能回数または再生可能時間をディスプレイ 2 3 に表示したり、再生ログをモデム 2 5 を 25 介して通信サーバ 2 1 6 や決済センター 1 1 0 等の外部機器へ送信することができる。さらに、プレーヤ 2 0 1 は聴取権データ 1 0 9 をモ

デム 2 5 を介して受信することも可能である。

ユーザが操作部 2 2 を操作することによって、媒体 1 内の所望のコンテンツの再生をシステムコントローラ 2 1 に指示する。再生せんとしているコンテンツが再生に関して無料のものであれば、セキュアデ

5 コーダ 2 0 2 を通ってアナログ出力が発生しても、メモリ部 1 6 に格納されている聴取権データ 1 0 9 が変更されない。若し、再生せんとしているコンテンツが再生する毎に課金される再生課金の対象のコンテンツである場合には、メモリ部 1 6 内の聴取権データ 1 0 9 が変更、例えば前述したように「- 1」だけ減算される。コンテンツが再

10 生される度、すなわちコンテンツデータが復号される毎に行われる課金処理としては、種々のタイプが可能である。この発明における課金処理としては、大きく分けて、買取型と、グロスに視聴料金をとるタイプと、セキュアデコーダ 2 0 2 でコンテンツデータに施されている暗号の復号化を行うごとに視聴料金を課する度数タイプとがある。買

15 取型は、コンテンツデータを一旦買い取った後では、コンテンツデータの再生処理に対して課金されないタイプである。グロスに視聴料金をとるタイプは、視聴料金をまとめて支払う月極めタイプ、コンテンツの視聴期間、コンテンツの視聴時間を限定するタイプ等である。

セキュアデコーダ 2 0 2 でコンテンツデータに施されている暗号の

20 復号化を行うごとに視聴料金を課す度数タイプとして、幾つかの形態が可能である。第 1 の形態は、予め設定された金額（プリペイドカード、電子マネー）または度数からコンテンツデータの再生処理の度に、金額または度数を減算するものである。コンテンツの再生にあたって残高または残り度数が不足する場合には、コンテンツの再生ができ

25 なくなる。第 2 の形態は、コンテンツデータの再生処理の度に、金額または度数が加算されるものである。予め設定した金額または度数に

累積金額または累積度数が達すると、コンテンツの再生ができなくなる。第3の形態は、コンテンツの再生時間に応じて、度数または金額が加算または減算されるものである。

上述した視聴料金を課す度数タイプで用いられる金額または度数は  
5、一定のものであっても良く、また、再生されるコンテンツの種類等に応じて金額または度数が重み付けされたものでも良い。課金処理は、コンテンツの1タイトル（音楽の例では、1曲）またはコンテンツの複数タイトル（音楽の例では、アルバム）と対応して行われる。

また、コンテンツデータの再生処理の定義の方法としては、コンテ  
10ンツ全体を再生した場合に、コンテンツが再生されたものとしても良いし、また、コンテンツの再生時間が所定時間以上の場合をコンテンツが再生をされたものとしても良い。さらに、普及・流通を促進するためのプロモーション用のコンテンツの再生に対しては課金されないようにしても良い。また、コンテンツの再生にあたって課金の対象と  
15なるコンテンツであっても、例えばコンテンツの先頭部分例えば先頭から10秒間のコンテンツ再生を無料としたり、コンテンツのハイライト部分のみの再生を無料としても良い。このように、コンテンツデータの再生処理に対して課金されるコンテンツと、コンテンツデータの再生処理が無料のコンテンツとが混在して例えば媒体1に記録され  
20ている場合に、コンテンツデータの再生処理、すなわち復号の際に付随データによって課金／無料が識別される。

付随データは、コンテンツデータ（圧縮符号化および暗号化されたコンテンツ例えばオーディオデータ）の前に付加されたデータである。付随データは、必要に応じて暗号化される。記録可能な媒体には、  
25付随データがコンテンツデータの前に付加されて媒体に記録されるか、または媒体1のデータ管理用領域に記録される。読み出し専用の媒

体の場合には、データ管理領域に付随データが記録される。光ディスクの場合では、一般的にディスクの最内周側の領域に管理領域が設けられており、この管理領域に各コンテンツデータに対応する付随データが記録される。メモ리카ードの場合には、例えば音楽データの1曲

5    を1ファイルとして扱うようにしたファイル管理データが規定され、ファイル管理データが記憶される記憶エリアに付随データが記憶される。

付随データには、再生にあたって課金されるコンテンツか、無料のコンテンツかを示す課金識別子、並びに課金処理が上述したような買

10    取型、グロス型、度数型等の課金タイプを区別し、各課金タイプにおける課金条件を指示する再生条件ラベルが含まれる。一例として、課金タイプが買取型の場合では、コンテンツデータの買取価格に関するデータが再生条件ラベルに記述され、課金タイプがグロス型の再生回数を制限する場合では、コンテンツの再生回数の上限等のデータが再

15    生条件ラベルに記述され、課金タイプがグロス型の再生期間を制限する場合では、コンテンツの再生期間のデータ（1日、1週間、1ヵ月等）が再生条件ラベルとして記述され、課金タイプが度数型の場合では、度数のデータ（1円／2分、1円／1分、1円／30秒、・・・）が再生条件ラベルとして記述される。さらに、再生にあたって課金

20    を前提としているコンテンツであっても、コンテンツを無料で視聴できる場合の条件を再生条件ラベルに記述することもできる。

付随データ中に、コンテンツデータの圧縮符号化の種類を示すための情報、暗号の種類および暗号のパラメータを示すための情報、チャンネル数の情報、ビットレートの情報等を記録しても良い。

25    付随データ中には、CD、MD、記録可能な光ディスク、不揮発性メモリを含むメモ리카ード等の媒体を一意に識別可能とするためのメ

ディアID例えばシリアル番号が含まれる。さらに、付随データ中には、デコーダIDが配置される。デコーダIDは、ユーザの端末、ユーザのプレーヤ201等に内蔵されているセキュアデコーダ202を一意に識別可能とするためのID例えばシリアル番号である。

- 5 次に、第7図のフローチャートを参照してプレーヤ201（第6図参照）においてなされる課金処理の一例について説明する。この処理は、セキュアデコーダ202内の制御部14およびプレーヤ201のシステムコントローラ21によって行われるものである。最初のステップS1は、媒体1に再生しようとするコンテンツデータが存在しているような再生スタンバイ状態である。具体的には、EMDにより配信されたコンテンツデータが媒体1に格納されている場合や媒体1に既にコンテンツデータが記録されている場合等が再生スタンバイに該当する。ステップS2では、ユーザが操作部22の再生ボタンを押すことによって再生指示がされたかどうか判定される。
- 10
- 15 ステップS2の結果が否定であることは、コンテンツデータのコピーの操作を意味するものと判定される。ステップS3において、無料再生用コンテンツデータのコピーか否かが判定される。無料再生用コンテンツデータとは、再生によって課金処理が行われないコンテンツを意味する。付随データ中に含まれる課金識別子を参照してステップ
- 20 S3の判定がなされる。無料再生用コンテンツであれば、著作権保護のために、セキュアデコーダ202からコンテンツデータに施されている暗号が復号化されたデータのコピー出力が禁止される（ステップS4）。

- 若し、無料再生用コンテンツデータのコピーでない、すなわち、課
- 25 金再生用コンテンツデータのコピーであるとステップS3で判定されると、課金再生用コンテンツデータのコピーデータがセキュアデコー

ダ 2 0 2 から出力される（ステップ S 5）。課金再生用コンテンツデータのコピーデータの出力は、セキュアデコーダ 2 0 2 から自由になされる。但し、ここで出力されるコピー出力、コピーデータは、付随データと暗号化、圧縮符号化がされたコンテンツデータである。

- 5     ステップ S 2 において、ユーザによって操作部 2 2 を用いて再生動作が指示されたものと判定されると、ステップ S 6 において、プレーヤ 2 0 1 のユーザに対して課金処理を受け入れるか否かが問われる。例えばプレーヤ 2 0 1 のディスプレイ 2 3 に課金処理が必要である旨のメッセージが表示され、ユーザがディスプレイ 2 3 の表示に基づいて操作部 2 2 の操作によって課金処理に対する回答をする。ユーザが課金処理を受け入れない場合には、コンテンツデータの無料再生ができない（ステップ S 7）。但し、付随データの再生条件ラベルによってコンテンツの部分的無料再生、例えばコンテンツとしての曲の先頭部分または曲のハイライト部分の再生を無料で行うことが許される場合もある。ユーザがコンテンツの再生に必要とされる課金処理を受け入れる場合には、ステップ S 8 において、ディスプレイ 2 3 上に、現に再生しようとするコンテンツの再生課金条件がユーザに対して提示される。このとき、ディスプレイ 2 3 には再生せんとしているコンテンツに対応する付随データ中の再生条件ラベルの情報に基づいて課金条件の提示がなされる。
- 10
- 15
- 20

- ステップ S 9 では、課金タイプが買取型かどうか判定される。課金タイプが買取型であれば、買取用の課金処理が行われる（ステップ S 1 0）。ステップ S 1 1 において、セキュアデコーダ 2 0 2 の復号器 1 1 では、サーバ 1 1 1 から送られてきた鍵データを使用してコンテンツデータに施されている暗号を復号し、ステップ S 1 2 において、コンテンツの無料再生を行う。この場合、無料再生するコンテンツ
- 25

のコピー出力が禁止される。但し、ムーブ処理、すなわち、コピーと異なり移動元となるプレーヤに移動対象となるコンテンツデータが再生可能な状態で残らず、移動先となるプレーヤ側でのみ移動対象となったコンテンツデータの復号、再生が可能となる処理は、行うことができる。

- 5       ステップS 9において、課金タイプが買取型でないと判定されると、ステップS 13において課金タイプがグロス型例えば月極型かどうか決定される。月極契約が存在し、課金タイプが月極型であるときには、ステップS 14において、再生せんとしているコンテンツが月極契約された楽曲か否かが判定される。ステップS 9で再生せんとしているコンテンツデータが月極契約されたコンテンツであれば、ステップS 15において、コンテンツの無料再生がなされる。この場合、課金再生用コンテンツのコピー出力はセキュアデコーダ202から自由に行うことができる。
- 10       ステップS 13において、課金タイプが月極型でないと判定されると、再生せんとしているコンテンツは、度数型で課金処理が行われるコンテンツであると判定される。ステップS 17において、再生せんとされているコンテンツデータに施されている暗号が復号され、ステップS 18において、コンテンツの課金再生がなされる。ステップS
- 15       18で行われる課金再生では、上述したように、コンテンツの再生の度数、再生時間等に応じて課金処理が行われる。課金再生用コンテンツのコピーは、セキュアデコーダ202から自由に出力されるので、利用者は自由にできる。さらに、ステップS 14において、月極契約の範囲内でない、すなわち再生動作が既に月極契約の範囲を超えていると判定された場合も、課金タイプが度数型の課金再生の処理（ステップS 17、ステップS 18）がなされる。
- 20
- 25

第8図は、聴取権データチャージャ204の一例の構成を示す。チャージャ204は、例えば持ち運び可能な可搬型の機器とされている。指示符号301がチャージャ全体を制御するCPUを示し、指示符号302が暗号化・復号化モジュールを示し、指示符号303がディスプレイ（例えば液晶ディスプレイ）を示し、指示符号304がユーザによって操作される複数のキーやボタンを示す。ディスプレイ303には、チャージャ204の動作に関連するメニュー、課金処理条件等が表示される。暗号化・復号化モジュール302は、プレーヤ201、決済センター110等との間で行われる再生ログ等の送信時の暗号化の処理と、聴取権データ109等の受信時の暗号の復号化の処理とを行う。指示符号305は、データチャージャ204の個別IDを示す。データチャージャ個別ID305は、例えば再生ログと共に例えば、決済センター110へ送信され、決済センター110側でデータチャージャ204と再生ログの対応関係が分かるようになされる。

例えば、第2図中の決済センター110との通信のために、モデム306およびUSB (Universal Serial Bus) 通信モジュール307が設けられている。データチャージャ204はモデム306によって、電話回線を介して決済センター110との通信が行われ、決済センター110から聴取権データ109を受け取り、決済センター110に対して再生ログを送信することができる。データチャージャ204は、USB通信モジュール307を使用し、パーソナルコンピュータおよびインターネットによって同様に決済センター110との通信が可能である。

決済センター110からデータチャージャ204が受信した聴取権データ109が聴取権データメモリ308に格納される。プレーヤ201のセキュアデコーダ202から受け取った再生ログがチャージャ

204の使用状況メモリ309に格納される。必要に応じてチャージャ204のログが再生ログに付加されたログデータが決済センター110へ送信される。尚、メモリ308および309は、電源オフとされても、その記憶内容が保持される不揮発性メモリである。

- 5 非接触通信モジュール310およびアンテナ311は、非接触でプレーヤ201との間で通信を行うためのものである。チャージャ204とプレーヤ201との間で行われる通信は、チャージャ204とプレーヤ201との間で相互に認証がされることを条件として、暗号化されたプロトコルを使用してなされる。プレーヤ201へはデータの
- 10 みならず、チャージャ204はプレーヤ201のセキュアデコーダ202が動作するのに必要な電力をプレーヤに送信可能とされている。したがって、プレーヤ201のメインの電源がオフであっても、聴取権データ109および再生ログの授受がセキュアデコーダ202との間で可能とされている。チャージャ204にはアンテナ311以外に
- 15 ライン接続用の端子も設けられている。なお、チャージャ204は非接触通信モジュール310およびアンテナ311またはラインを使用して聴取権データ販売端末206との通信を行う。

- 第9図は、セキュアデコーダ202のより詳細な構成、すなわち、課金処理に関する機能的構成を示す。第9図に示される構成のうち、
- 20 第8図に示される構成要素と共通する部分には、第8図で用いられた指示符号と同一符号を付して示す。媒体1から読み出された暗号化され、且つ圧縮符号化されたコンテンツデータと付随データとからなる再生データが復号器11に供給される。復号器11には、媒体1を一意に識別可能とするためのメディア個別IDもコンテンツデータ、付
- 25 随データとともに供給される。復号器11によってコンテンツデータ、付随データに施されている暗号の復号がなされる。

- 復号器 1 1 の出力データが再生条件ラベル検出部 4 0 1 に供給され、付随データ中の再生条件ラベルが検出される。検出された再生条件ラベルがセキュアデコーダ 2 0 2 の処理に使用される。復号器 1 1 によって暗号の解かれたデータ、すなわち出力データは伸張器 1 2 に供給され、伸張器 1 2 で圧縮符号化の復号がなされる。伸張器 1 2 で伸張処理されたデジタルデータがウォーターマーク検出部 4 0 2 に供給される。ウォーターマーク検出部 4 0 2 は、後述するようにコンテンツデータがアナログ信号に変換されてデコーダ 2 0 4 からの出力時に付加されているウォーターマークを検出し、検出されたウォーター
- 10 マークと再生条件ラベルとに基づいて、付随データの再生条件ラベルが改ざんされたか否かをチェックする。例えばウォーターマークが検出できなかったり、検出されたウォーターマークが本来検出されるべきウォーターマークの形態とは異なっている場合には再生条件ラベルが改ざんされたと判定する。
- 15 指示符号 4 0 3 は、聴取権カウンタを示す。聴取権カウンタ 4 0 3 においては、コンテンツデータを復号する度に、聴取権データ 1 0 9 に対して変更を加える。例えばメモリ部 1 6 に格納されている聴取権データ 1 0 9、例えば度数データを「-1」だけ減算する処理を行う。メモリ部 1 6 に格納される聴取権データ 1 0 9 は、アンテナ 1 8（
- 20 またはライン）と通信モジュール 1 7 とによって、上述した聴取権データチャージャ 2 0 4 から送信されたものである。通信モジュール 1 7 内には、再生ログ等の送信時の暗号化と、聴取権データ 1 0 9 の受け取り時の復号化のためのモジュールが設けられている。なお、この発明ではコンテンツデータとして楽曲データを取り扱う例を用いて説
- 25 明を行っているので、聴取権の用語を使用しているが、映像データを含めて考えた時には、聴取権の代わりに視聴権の用語が使用される。

聴取権カウンタ 4 0 4 において、聴取権に関する処理がされると、ウォーターマーク付加部 4 0 4 において、セキュアデコーダ 2 0 2 から出力されるデータに対してウォーターマークが付加される。付加部 4 0 4 で新たに付加されるウォーターマークは、コンテンツデータとしての楽曲データに存在する冗長な部分例えば出力されるオーディオデータの下位のビットを利用することでウォーターマークを付加できる。このようにオーディオデータの下位のビットに付加されたウォーターマークは、アナログ信号に変換しても残り、且つウォーターマークを除去することが不可能か、非常に困難なものである。付加部 4 0 4 で付加されるウォーターマークは、再生条件ラベルの全体または一部のデータと、デコーダ個別 I D 4 0 5 の情報を含むものである。ウォーターマークが付加されたデジタルデータが D/A 変換器 1 3 によってアナログ信号に変換され、セキュアデコーダ 2 0 2 から外部へ出力される。上述したウォーターマーク検出部 4 0 2 は、このように付加されたウォーターマークを検出するものである。

セキュアデコーダ 2 0 2 が I C カードのインターフェースを持ち、また、聴取権データチャージャ 2 0 4 が決済センター 1 1 0 または金融会社から電子マネーを受け取り、受け取った電子マネーをセキュアデコーダ 2 0 2 が備えているインターフェースを介して I C カードに記録するようにしても良い。すなわち、セキュアデコーダ 2 0 2 に聴取権データ 1 0 9 の書き込みに対して、オプションなものとして電子マネーの記録装置としての機能を持たせることができる。

聴取権カウンタ 4 0 3 によってなされる課金処理の概略を説明する。一例として、課金処理が課金タイプとしての度数型で行われる場合に適用される例について説明する。すなわち、聴取権データとして予め設定された度数からコンテンツデータとしての楽曲データの再生処

理の度に、一律またはコンテンツデータ毎に定められた度数を減算したり、楽曲一タの再生処理の度に、度数が加算されたり、楽曲データの再生時間に応じて、度数が加算または減算される。例えば付随データから再生条件ラベル検出部 4 0 1 によって再生条件ラベルが抜き出  
5 される。再生条件ラベルには、課金条件が含まれている。この課金条件をもとに上述した聴取権データとして設定された度数からの減算または度数のカウントアップが行われる。コンテンツデータとしての楽曲データが伸張器 1 2 から出力されている期間を 3 0 秒、1 分等の単位時間によって計測し、計測された時間の長さに対して課金される課  
10 金処理を行ってもよい。すなわち、この場合の課金処理では単位時間が一つの度数に対応される。

計測された時間と再生条件ラベルに基づいて、聴取権カウンタ 4 0 3 によって度数が制御される。すなわち、ラベル検出部 4 0 1 によって抜き出された再生条件ラベルを参照して、カウンタ 4 0 3 はメモリ  
15 部 1 6 に格納されている聴取権データ 1 0 9 に対して減算または加算処理を行い、メモリ部 1 6 内の聴取権データ 1 0 9 を書き換える。再生時間または再生期間を課金条件としている場合には、図示しないタイマー／カレンダーを用いてコンテンツの再生時間の累積処理またはコンテンツの再生が行われている日時と再生可能期限との照合処理が  
20 カウンタ 4 0 3 で行われる。

聴取権カウンタ 4 0 3 または他の制御部は、さらに、コンテンツが再生可能かどうかを判断する。カウンタ 4 0 3 は、例えばコンテンツを再生する度に聴取権データとして設定されている度数を減算して、  
25 度数の残りが「0」となると、コンテンツの新たな再生を不可能と判断する。カウンタ 4 0 3 は聴取権データとしての累積度数が設定された度数に到達したり、コンテンツの再生時間の累積値が設定された時

間に到達したり、コンテンツの再生を行わんとしている日時が再生期限を越えたりすると、上述した場合と同様に、コンテンツの新たな再生を不可能と判断する。カウンタ 4 0 3 が再生可能と判定している場合には、セキュアデコーダ 2 0 2 から楽曲データが出力され、一方  
5 、カウンタ 4 0 3 によって再生不可能と判定された場合には、セキュアデコーダ 2 0 2 から楽曲データの出力が禁止される。

この発明の一実施形態では、上述した決済センター 1 1 0 または聴取権データ販売機 2 0 6 から聴取権データチャージャ 2 0 4 に聴取権データ 1 0 9 を渡す場合、並びに聴取権データチャージャ 2 0 4 から  
10 プレーヤ 2 0 1 に聴取権データ 1 0 9 を渡す場合において、セキュリティを高くするために、発行元または管理者である決済センター 1 1 0 がセキュリティ、例えば、用いる暗号を定期的または非定期で変更可能とするものである。

第 1 0 図 A, B は、聴取権データ 1 0 9 を渡す時のデータフォーマットの一例を示す。勿論、決済センター 1 1 0 から送信される聴取権データに代えて、第 1 0 図 A, B に示すフォーマットを踏襲した電子マネーが決済センター 1 1 0 から送信されても良い。第 1 0 図 A が 1  
15 フレーム (2 5 6 ビット) の構成を示す。フレームの先頭にヘッダ (1 6 ビット) が位置する。ヘッダの次に、開始年月日 (YMD) (2 4 ビット) と終了年月日 (YMD) とが順に配置される。この開始年月日 (YMD) と終了年月日 (YMD) とによって聴取権データ 1 0 9 の有効な期間がこれらのデータによって規定される。開始年月日、  
20 終了年月日の年が 1 5 ビットのバイナリ表記で表され、月および日がそれぞれ 4 ビットおよび 5 ビットのバイナリ表記で表される。開始年月日または終了年月日を決めていない場合には、2 4 ビットを全て 0  
25 のビットとする。例えば、聴取権データ 1 0 9 の有効期間を予め定め

ておくことによって、終了年月日を明示しなくても良い。

終了年月日 (YMD) に続いて6ビットのタイプが聴取権データに施されている暗号化の種類を表す。DES (Data Encryption Standard) による暗号化、RSAによる暗号化等が使用できる。DESは、平  
 5 文をブロック化し、ブロック毎に暗号変換を行うブロック暗号の一つである。DESは、64ビットの入力に対して64ビット (56ビットの鍵と8ビットのパリティ) のキーを用いて暗号変換を行い、64ビットを出力する。DESは、暗号化と復号化に同一の鍵データを使う共通鍵方式であり、RSAは、暗号化と復号化に異なる鍵データを使う公開鍵暗号の一つである。これら以外の暗号を使用することもで  
 10 きる。

暗号化の種類情報の後に、10ビットの鍵長が配される。鍵長は、暗号化を復号するための鍵の長さを示す。鍵長の後に鍵 (第10図Aの例では、1024ビット) が配置される。32ビットのEDC (エ  
 15 ラー検出コード) 用の鍵と、それに続いて256ビットの暗号化された聴取権データMPが配される。

データMPの後に64ビットのEDCと128ビットのECC (エラー訂正コード) とが順に配置され、1フレームのデータ配置が完結する。EDCとして、CRC (cyclic redundancy code) 等が使用さ  
 20 れ、ECCとして、例えば (198, 182, 17) のリードソロモンコード (Reed-Solomon code) が使用される。ECCは、ヘッダから始まり、EDCまでのデータのエラーの有無を検出する。EDCは、開始年月日 (YMD) から始まって聴取権データMPまでのエラーを訂正する。

25 EDCの多項式として、例えば  $(x^{16} + x^{12} + x^5 + x + 1) (x^{16} + x + 1) (x^{32} + \_\_ x^{31} + \_\_ x^{30} \cdots + \_\_ x^4 + \_\_ x^3 + \_\_$

- $x^2 + \underline{\quad} x + 1$ ) を使用する時に、下線部分の係数の値が EDC 用鍵 (64 ビット) に配されている。したがって、聴取権データ MP に施されている暗号化を復号するためには、ECC によるエラー訂正を行い、EDC 用の鍵を得、次に、EDC によるエラー検出を行い、エラー検出の結果が OK (エラー無し) であれば、聴取権データ MP を復号できる。このようにして、暗号化された聴取権データ MP のセキュリティを高くすることができる。さらに、必要に応じて、全体的にスクランブル (例えば最大長周期 (M) 系列を使用したランダム化) を行うようにしても良い。
- 10 第 10 図 B は、聴取権データ 109 の送信のための他のデータ構成例を示す。第 10 図 A に示すデータ配列 (影を付けて示す) の後に暗号化を行うためのソフトウェア (例えば 4 M ビット) が配され、さらに、暗号化のソフトウェアに対する EDC ソフトウェア (例えば 1 M ビット) が配される。EDC ソフトウェアは、例えば 2 K バイト単位
- 15 で ECC ブロック化されている。第 10 図 B のデータ構成は、暗号化の復号用ソフトウェアも一緒に送るようにしたものである。
- 上述した聴取権データ 109 の伝送フォーマットは、重要な部分が 256 ビットのみであるが、その部分が暗号化、EDC、ECC により守られている。それによって、聴取権データ 109 を不正に入手したり、改ざんすることを防止できる。さらに、この発明の一実施形態
- 20 では、第 10 図 A に示すフォーマットにおける開始年月日 (YMD)、鍵長、鍵、EDC 用鍵の内の少なくとも 1 つを決済センター 110 が定期的に、或いは非定期的に変更可能としている。それによって、聴取権データ 109 が改ざんされたり、不正利用される疑いがある時
- 25 、または改ざんや不正使用を未然に防ぐことができる。例えば聴取権データ 109 の暗号化の解読方法がインターネット上で公開されるよ

うな事態にも直ちに対処することができる。第10図Bに示すフォーマットでは、さらに、暗号化ソフトウェアおよび／またはEDCソフトウェアを変更することができるので、聴取権データのセキュリティを強力とすることができる。

- 5      このように、聴取権データ109のセキュリティを変更した後では、古いセキュリティの聴取権データ109が無効となり、古い聴取権データ109では、コンテンツを利用できない、すなわちコンテンツデータの復号によりコンテンツの再生が行えない。この場合、使えなくなった古い聴取権データ109を所有している者は、古い聴取権データ109を新たな聴取権データ109へ交換すること決済センター
- 10      110に要求することができる。このように改ざんが発覚した時点で上述した開始年月日（YMD）等を変更する交換システムの代わり、またはこの交換システムに加えて、ユーザがコンテンツの再生によって聴取権データを使い切ったり、残量が少なくなり、新たに聴取権データ
- 15      109を入手する時に、残っている古い聴取権データが新しい聴取権データに自動的に交換されるシステムが採用するようにしてもよい。

- 第11図は、コンテンツの再生と聴取権データ109のセキュリティとが連携した処理を示すフローチャートである。一例として、聴取権データ109のセキュリティが1年に1回定期的に変更される場合
- 20      を説明する。ステップS1において、暗号化コンテンツの再生を行おうとすると、聴取権データ109が1年以内かどうかステップS2で判定される。セキュアデコーダ202がカレンダーを内蔵しており、第10図Aに示した聴取権データの開始年月日（YMD）に基づいてステップS2の判定を行うことができる。この場合、例えば、ステ
- 25      ップS2で1年に対してある程度の周知期間 $\alpha$ を付加し、期間（1年＋ $\alpha$ ）を経過した時に聴取権データを無効とするように判定しても良

い。

聴取権データが1年以上経過しているとステップS 2で判定された場合には、コンテンツの再生が停止する（ステップS 3）。ステップS 2で1年以内の聴取権データと判定された場合には、聴取権データ  
5 がコンテンツの再生、すなわちコンテンツデータの復号を行うために必要とされる最低単位（a）以上かどうかステップS 4で判定される。ステップS 4で最低単位の聴取権データが残っていない場合には、再生処理が停止し、その旨のメッセージがプレーヤ201のディスプレイ23に表示される（ステップS 5）。メッセージが表示される  
10 代わりに音声のメッセージを発生してもユーザに告知しらしめるようにしても良い。ステップS 3においても同様に、ステップS 5と同様にメッセージをユーザに提示するようにしても良い。

ステップS 4において、聴取権データがコンテンツ再生に必要とされる最低単位a以上残っていると判定されると、聴取権データの1単位が消費される。聴取権データが実際に消費されたかどうかステップ  
15 プS 6において監視される。例えば、聴取権データの消費する前の状態と、消費した後の状態とが比較される。例えば、聴取権データとして設定された度数が再生課金の課金条件に基づいて「-1」等の所定の値だけ正しく減算されたか否かが判定される。若し、不正な改ざん  
20 等によって、聴取権データが消費されないときは、ステップS 5に進み、コンテンツの再生停止、ユーザへのメッセージの提示に移行する。ステップS 6において、聴取権データの消費が確認できると、ステップS 7において、コンテンツデータに施されている暗号が復号され、前述したようにコンテンツが再生される。ステップS 3またはステ  
25 ップS 5で行われるコンテンツの再生の停止、ユーザに対する警告等のメッセージの提示と共に、またはこれらステップS 3、S 5の処理

に代えて、決済センター 110 に対して、セキュアデコーダ 202 よりまたはプレーヤ 201 から聴取権データのセキュリティチェックの結果が正しくないことを通知するようにしても良い。

- コンテンツの再生が終了したかどうかステップ S 8 において判定  
5 される。コンテンツの再生の終了は、通常は、ユーザが再生のプレーヤ 201 の操作部 22 のキー操作により停止指示を行うことでなされる。コンテンツの再生が継続する限り、ステップ S 4 ~ S 8 の処理が繰り返される。例えばユーザがコンテンツを再生している時間に応じて、上述したように聴取権データが消費、例えば度数が減算処理される。  
10 る。ステップ S 8 において、コンテンツの再生が終了したものと判定されると、再生処理が終了する（ステップ S 9）。第 11 図の例は、再生時間の単位時間に応じて聴取権データが減少する課金処理であるが、前述したような再生時間に応じて度数が加算される場合でも、同様にこの発明を適用できる。
- 15 また、利用または再生せんとするコンテンツ例えば楽曲データが付随データ中に年月日データ持ち、楽曲データと聴取権データとの間で、互いに年月日データをカウンタ 403 等で照合し、聴取権データの年月日に応じて利用または再生せんとするコンテンツが再生可能なコンテンツであるか否かを識別することもできる。
- 20 さらに、聴取権データの改ざん等が発覚した際に聴取権データの書き換えを行う代わりに決済センターの指示により、新旧の聴取権データの入れ替えを行うようにしても良い。例えば 10000 度数（ポイント）が入るデータチャージャの場合で、残りが 3000 度数で、5000 度を補充して欲しい時に、残りを含めた（3000 + 5000）  
25 0）度を新たな聴取権データとするようにしても良い。よりさらに、再生ログをプレーヤからデータチャージャに伝送するシステムにお

いては、不正に聴取を行って、再生ログが予め定められた許容量を越え  
ると、聴取権データを無効にする等してそのプレーヤによるコンテ  
ンツの再生を禁止するようにできる。そのような事態が生じた時に、  
データチャージャから自動的に決済センターに連絡がなされる。その  
5 連絡時に、データチャージャはプレーヤに残っている聴取権データ全  
てを吸い上げるようにしても良い。よりさらに、再生ログを決済セン  
ターで収集するシステムでは、電子マネー、電子利用権をユーザに送  
信した履歴と、ユーザ側から吸い上げた再生ログの使用履歴とを比較  
することによって、ユーザが不正利用を行っていないかどうかを発見  
10 するようにしても良い。

なお、上述した実施形態では、主として再生されるコンテンツとし  
てオーディオコンテンツについて説明したが、オーディオ以外のビデ  
オデータ、静止画像データ、文字データ、コンピュータグラフィック  
データ、ゲームソフトウェア、およびコンピュータプログラム等のコ  
15 ンテンツに対しても、上述したのと同様にこの発明を適用することが  
できる。

以上の説明から明らかなように、この発明によれば、セキュリティ  
を変更するので、電子マネー、電子利用権のセキュリティを向上する  
ことができる。例えば偽造の電子マネー、電子利用権が出回ったり、  
20 不正利用方法が公開されたりしても、直ちに対応することができる。  
また、定期的にセキュリティを変更することによって、不正利用、偽  
造のおそれを未然に防ぐことができる。さらに、セキュリティチェッ  
クの結果が正しくない時には、コンテンツの利用を禁止することで、  
電子マネー、電子利用権のみならず、コンテンツの著作権を強力に保  
25 護することができる。よりさらに、再生ログを収集するシステムでは  
、渡した電子マネー、電子利用権と再生ログから不正を発見すること

ができる。

## 請求の範囲

1. 現金に相当する効力を有する電子マネーであって、  
そのセキュリティを発行元または管理者が変更可能とされたことを  
特徴とする電子マネー。
- 5     2. 上記セキュリティが暗号化の鍵、上記鍵の鍵長、エラー検出お  
よび／または訂正コード、または有効期間である請求の範囲第1項記  
載の電子マネー。
3. 上記変更が所定期間毎になされる請求の範囲第1項記載の電子  
マネー。
- 10    4. 上記変更が上記発行元または管理者の必要に応じてなされる請  
求の範囲第1項記載の電子マネー。
5. 上記変更がなされた後、一定期間経過後に上記変更前のものを  
無効とする請求の範囲第1項記載の電子マネー。
6. コンテンツの再生等のソフトウェアの利用を可能とする電子利  
15    用権であって、  
そのセキュリティを発行元または管理者が変更可能とされたことを  
特徴とする電子利用権。
7. 上記セキュリティが暗号化の鍵、上記鍵の鍵長、エラー検出お  
よび／または訂正コード、または有効期間である請求の範囲第6項記  
20    載の電子利用権。
8. 上記変更が所定期間毎になされる請求の範囲第6項記載の電子  
利用権。
9. 上記変更が上記発行元または管理者の必要に応じてなされる請  
求の範囲第6項記載の電子利用権。
- 25    10. 上記変更がなされた後、一定期間経過後に上記変更前のもの  
を無効とする請求の範囲第6項記載の電子利用権。

1 1. 上記ソフトウェアは、オーディオデータ、ビデオデータ、静止画像データ、文字データ、コンピュータグラフィックデータ、ゲームソフトウェア、およびコンピュータプログラムの内の少なくとも1つである請求の範囲第6項記載の電子利用権。

- 5 1 2. 圧縮符号化および／または暗号化されたソフトウェアが配布され、配布されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子マネーを介して課金処理がなされるようにした課金システムであって、

電子マネーのセキュリティを発行元または管理者が変更可能とされたことを特徴とする課金システム。

1 3. 上記セキュリティが暗号化の鍵、上記鍵の鍵長、エラー検出および／または訂正コード、または有効期間である請求の範囲第12項記載の課金システム。

- 1 4. 上記変更が所定期間毎になされる請求の範囲第12項記載の課金システム。

1 5. 上記変更が上記発行元または管理者の必要に応じてなされる請求の範囲第12項記載の課金システム。

1 6. 上記変更がなされた後、一定期間経過後に上記変更前のものを無効とする請求の範囲第12項記載の課金システム。

- 20 1 7. 上記システムは、ユーザが所有する電子マネーまたは電子利用権を上記発行元または管理者が買い取るか、または有効な電子マネーまたは電子利用権へ交換する請求の範囲第12項記載の課金システム。

- 25 1 8. 上記システムは、ユーザの復号の結果が電子マネーまたは電子利用権で許容された範囲に達したタイミングで、電子マネーまたは電子利用権の要求を発生する請求の範囲第12項記載の課金システム

。

19. 上記ソフトウェアは、オーディオデータ、ビデオデータ、静止画像データ、文字データ、コンピュータグラフィックデータ、ゲームソフトウェア、およびコンピュータプログラムの内の少なくとも1  
5 つである請求の範囲第12項記載の課金システム。

20. 圧縮符号化および／または暗号化されたソフトウェアが配布され、配布されたソフトウェアをユーザが復号するに際し、ユーザが所有する電子利用権を介して課金処理がなされるようにした課金システムであって、

10 電子利用権のセキュリティを発行元または管理者が変更可能とされたことを特徴とする課金システム。

21. 上記セキュリティが暗号化の鍵、上記鍵の鍵長、エラー検出および／または訂正コード、または有効期間である請求の範囲第20項記載の課金システム。

15 22. 上記変更が所定期間毎になされる請求の範囲第20項記載の課金システム。

23. 上記変更が上記発行元または管理者の必要に応じてなされる請求の範囲第20項記載の課金システム。

24. 上記変更がなされた後、一定期間経過後に上記変更前のものを無効とする請求の範囲第20項記載の課金システム。  
20

25. 上記システムは、ユーザが所有する電子マネーまたは電子利用権を上記発行元または管理者が買い取るか、または有効な電子マネーまたは電子利用権へ交換する請求の範囲第20項記載の課金システム。

26. 上記システムは、ユーザの復号の結果が電子マネーまたは電子利用権で許容された範囲に達したタイミングで、電子マネーまたは

電子利用権の要求を発生する請求の範囲第 20 項記載の課金システム。  
。

27. 上記ソフトウェアは、オーディオデータ、ビデオデータ、静止画像データ、文字データ、コンピュータグラフィックデータ、ゲームソフトウェア、およびコンピュータプログラムの内の少なくとも 1  
5 つである請求の範囲第 20 項記載の課金システム。

28. 電子マネーまたは電子利用権を用いることによって稼働しているシステムであって、

電子マネーまたは電子利用権のセキュリティチェックを行い、  
10 セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システム。

29. 上記セキュリティチェックが暗号化の復号の結果、エラー検出および／または訂正の結果、または有効期間のチェックである請求  
15 の範囲第 28 項記載の課金システム。

30. 上記セキュリティチェックは、復号がされた後に残りの電子マネーまたは電子利用権が正しい状態かどうかをチェックすることでなされる請求の範囲第 28 項記載の課金システム。

31. 上記通知が電子マネーまたは電子利用権の発行元または管理  
20 者に対してなされる請求の範囲第 28 項記載の課金システム。

32. 上記通知がユーザに対してなされる請求の範囲第 28 項記載の課金システム。

33. 圧縮符号化および／または暗号化されたソフトウェアが配布され、配布されたソフトウェアをユーザが復号するに際し、ユーザが  
25 所有する電子マネーまたは電子利用権を介して課金処理がなされるようにした課金システムであって、

- 電子マネーまたは電子利用権のセキュリティチェックを行い、  
セキュリティチェックの結果が正しくないときには、システムの稼働の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする課金システム。
- 5     34. 上記セキュリティチェックが暗号化の復号の結果、エラー検出および／または訂正の結果、または有効期間のチェックである請求の範囲第33項記載の課金システム。
35. 上記セキュリティチェックは、復号がされた後に残りの電子マネーまたは電子利用権が正しい状態かどうかをチェックすることで
- 10    なされる請求の範囲第33項記載の課金システム。
36. 上記通知が電子マネーまたは電子利用権の発行元または管理者に対してなされる請求の範囲第33項記載の課金システム。
37. 上記通知がユーザに対してなされる請求の範囲第33項記載の課金システム。
- 15    38. 配布された圧縮符号化および／または暗号化されたソフトウェアを復号するに際し、電子マネーまたは電子利用権を介して課金処理がなされるようにした情報処理装置であって、
- 電子マネーまたは電子利用権のセキュリティチェックを行い、  
セキュリティチェックの結果が正しくないときには、ソフトウェア
- 20    の復号の停止、並びにセキュリティチェックの結果が正しくないことの通知の少なくとも一方を行うことを特徴とする情報処理装置。
39. 上記セキュリティチェックが暗号化の復号の結果、エラー検出および／または訂正の結果、または有効期間のチェックである請求の範囲第38項記載の情報処理装置。
- 25    40. 上記セキュリティチェックは、復号がされた後に残りの電子マネーまたは電子利用権が正しい状態かどうかをチェックすることで

なされる請求の範囲第 3 8 項記載の情報処理装置。

4 1. 上記通知が電子マネーまたは電子利用権の発行元または管理者に対してなされる請求の範囲第 3 8 項記載の情報処理装置。

4 2. 上記通知がユーザに対してなされる請求の範囲第 3 8 項記載  
5 の情報処理装置。

4 3. 圧縮および／または暗号化されたコンテンツデータを再生処理する際に電子利用権のセキュリティをチェックし、

上記セキュリティチェックの結果、上記電子利用権が有効でない場合には上記コンテンツデータの再生を中止し、

10 上記セキュリティチェックの結果、上記電子利用権が有効であった場合には上記コンテンツデータの再生処理を行うとともに上記電子利用権を消費するコンテンツデータの再生方法。

4 4. 上記方法は、上記セキュリティチェックの結果、上記電子利用権が有効であった場合には上記電子利用権が上記コンテンツデータの再生処理に必要な量だけ残っているのか否かを判別し、上記コンテンツデータの再生処理に必要な量だけ残っていないときには、上記コンテンツデータの再生処理を行う請求の範囲第 4 3 項記載のコンテンツデータの再生方法。  
15

4 5. 上記方法は、上記コンテンツデータの再生処理に必要な量だけ残っていると判別されたときには、上記コンテンツデータの再生処理を行うとともに上記電子利用権を消費する請求の範囲第 4 4 項記載のコンテンツデータの再生方法。  
20

4 6. 上記方法は、上記電子利用権の消費を上記コンテンツデータに付随する付随データ中の課金条件に基づいて行われる請求の範囲第  
25 4 3 項記載のコンテンツデータの再生方法。

4 7. 上記電子利用権には、ヘッダと少なくとも有効開始年月日に

関するデータと暗号化の種類を示すデータと電子利用権に関するデータとを含むとともにエラー訂正コードを有する請求の範囲第 4 3 項記載のコンテンツデータの再生方法。

4 8. 上記方法は、上記セキュリティチェックの結果、上記電子利用権が有効でないと判定されたときには、上記電子利用権を管理する管理機構にその旨通知する請求の範囲第 4 3 項記載のコンテンツデータの再生方法。

4 9. 圧縮および／または暗号化されたコンテンツデータを再生処理にあたって行われる課金処理に用いられる電子利用権のセキュリティを10 チェックし、

上記セキュリティチェックの結果、上記電子利用権が有効でない場合には上記コンテンツデータの再生を中止し、

上記セキュリティチェックの結果、上記電子利用権が有効であった場合には上記コンテンツデータの再生処理を行うとともに上記電子利用権に基づき課金処理を行うコンテンツデータの再生方法。15

5 0. 上記方法は、上記セキュリティチェックの結果、上記電子利用権が有効であった場合には上記電子利用権が上記コンテンツデータの再生処理に必要な量だけ残っているのか否かを判別し、上記コンテンツデータの再生処理に必要な量だけ残っていないときには、上記コンテンツデータの再生処理を行う請求の範囲第 4 9 項記載のコンテンツデータの再生方法。20

5 1. 上記方法は、上記コンテンツデータの再生処理に必要な量だけ残っていると判別されたときには、上記コンテンツデータの再生処理を行うとともに上記電子利用権に基づき課金処理を行う請求の範囲第 5 0 項記載のコンテンツデータの再生方法。25

5 2. 上記方法は、上記電子利用権に基づく課金処理は上記コンテ

ンツデータに付随する付随データ中の課金条件に基づいて行われる請求の範囲第 4 9 項記載のコンテンツデータの再生方法。

5 3. 上記電子利用権には、ヘッダと少なくとも有効開始年月日に関するデータと暗号化の種類を示すデータと電子利用権に関するデータとを含むとともにエラー訂正コードを有する請求の範囲第 4 9 項記載のコンテンツデータの再生方法。

5 4. 上記方法は、上記セキュリティチェックの結果、上記電子利用権が有効でないと判定されたときには、上記電子利用権を管理する管理機構にその旨通知する請求の範囲第 4 9 項記載のコンテンツデータの再生方法。

5 5. 上記方法は、上記電子利用権を補填する際に新旧の電子利用権を書き換える請求の範囲第 4 9 項記載のコンテンツデータの再生方法。

5 6. 上記方法は、上記電子利用権を補填する際に再生されたコンテンツデータの再生履歴に関するデータを上記電子利用権を管理する管理機構に送信する請求の範囲第 4 3 項記載のコンテンツデータの再生方法。

5 7. 管理機構から購入した電子利用権をプレーヤ内のメモリに記憶し、プレーヤによって圧縮および／または暗号化されたコンテンツデータを再生処理にあたって行われる課金処理に用いられる上記電子利用権のセキュリティをチェックし、

上記セキュリティチェックの結果、上記電子利用権が有効でない場合には上記コンテンツデータの再生を中止し、

上記セキュリティチェックの結果、上記電子利用権が有効であった場合には上記コンテンツデータの再生処理を行うとともに上記電子利用権に基づき課金処理を行う再生制御方法。

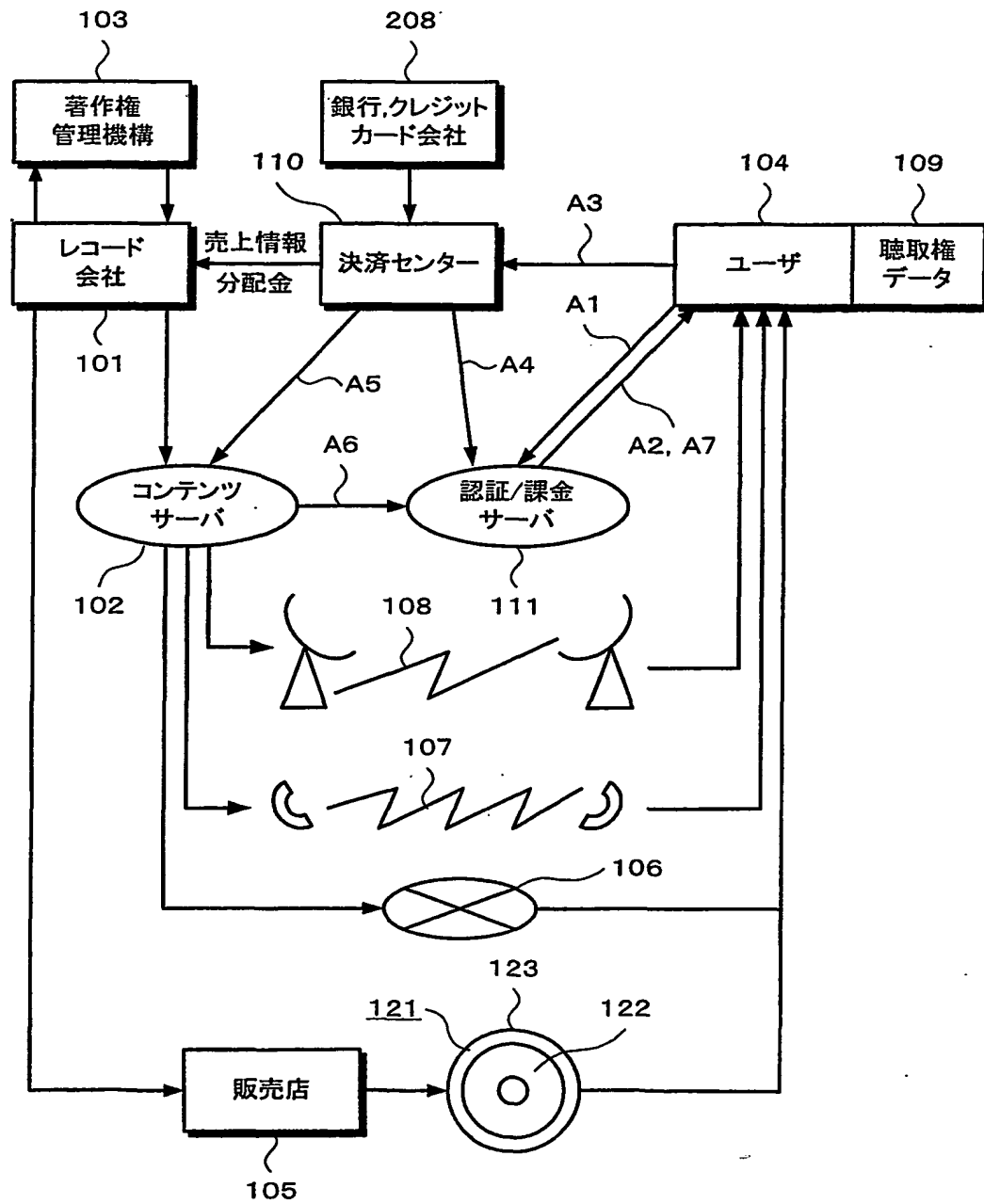
58. 上記方法は、上記電子利用権を補填する際に新旧の電子利用権を書き換える請求の範囲第57項記載の再生制御方法。

59. 上記方法は、上記電子利用権を補填する際に再生されたコンテンツデータの再生履歴に関するデータを上記電子利用権を管理する  
5 上記管理機構に送信する請求の範囲第57項記載の再生制御方法。

60. 上記管理機構は、上記再生履歴が予め定められた許容量を超えているときには上記プレーヤによるコンテンツデータの再生を禁止する請求の範囲第59項記載の再生制御方法。

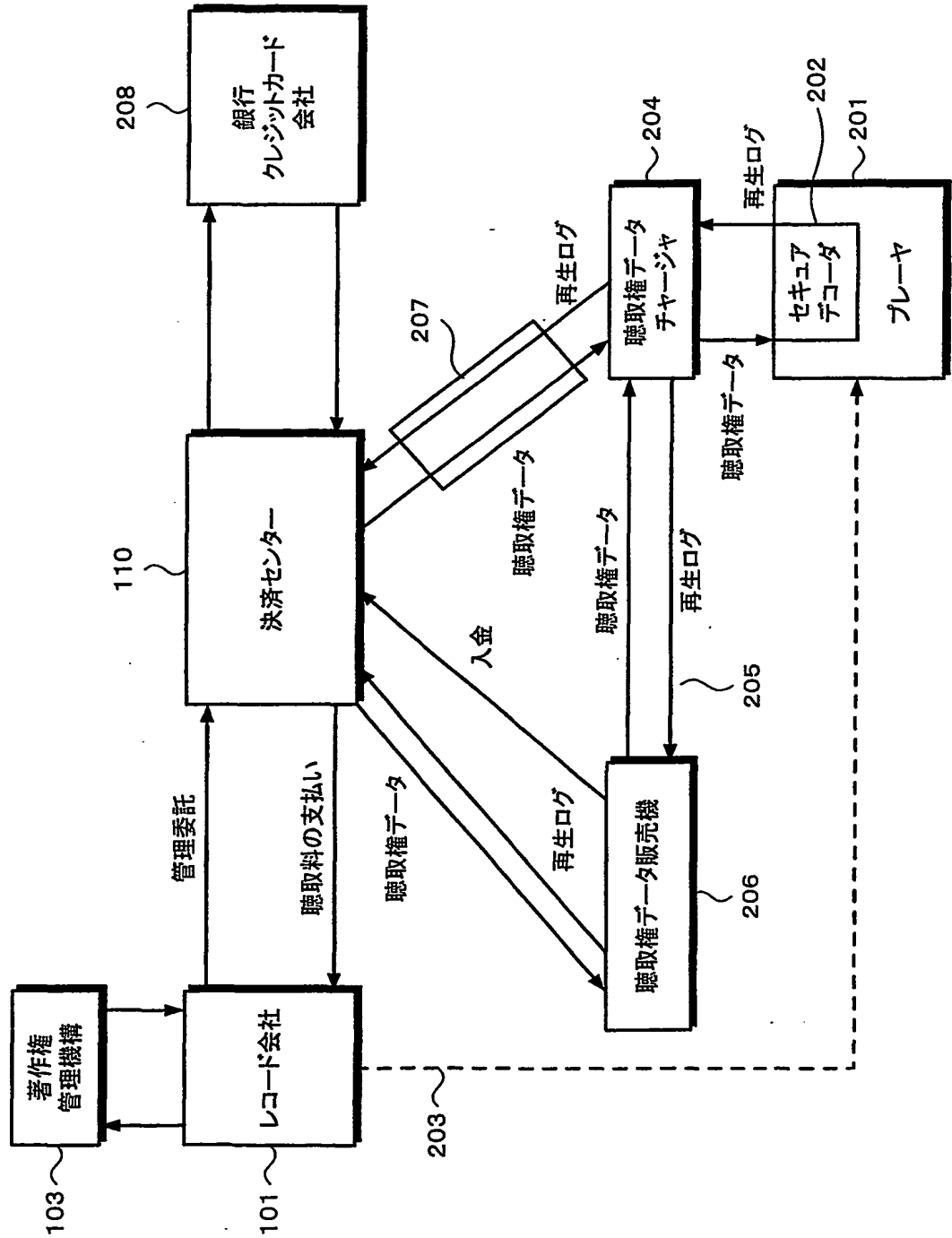
61. 上記管理機構は、更に上記プレーヤのメモリに記憶されている電子利用権を吸い上げる請求の範囲第60項記載の再生制御方法。  
10

## 第1図



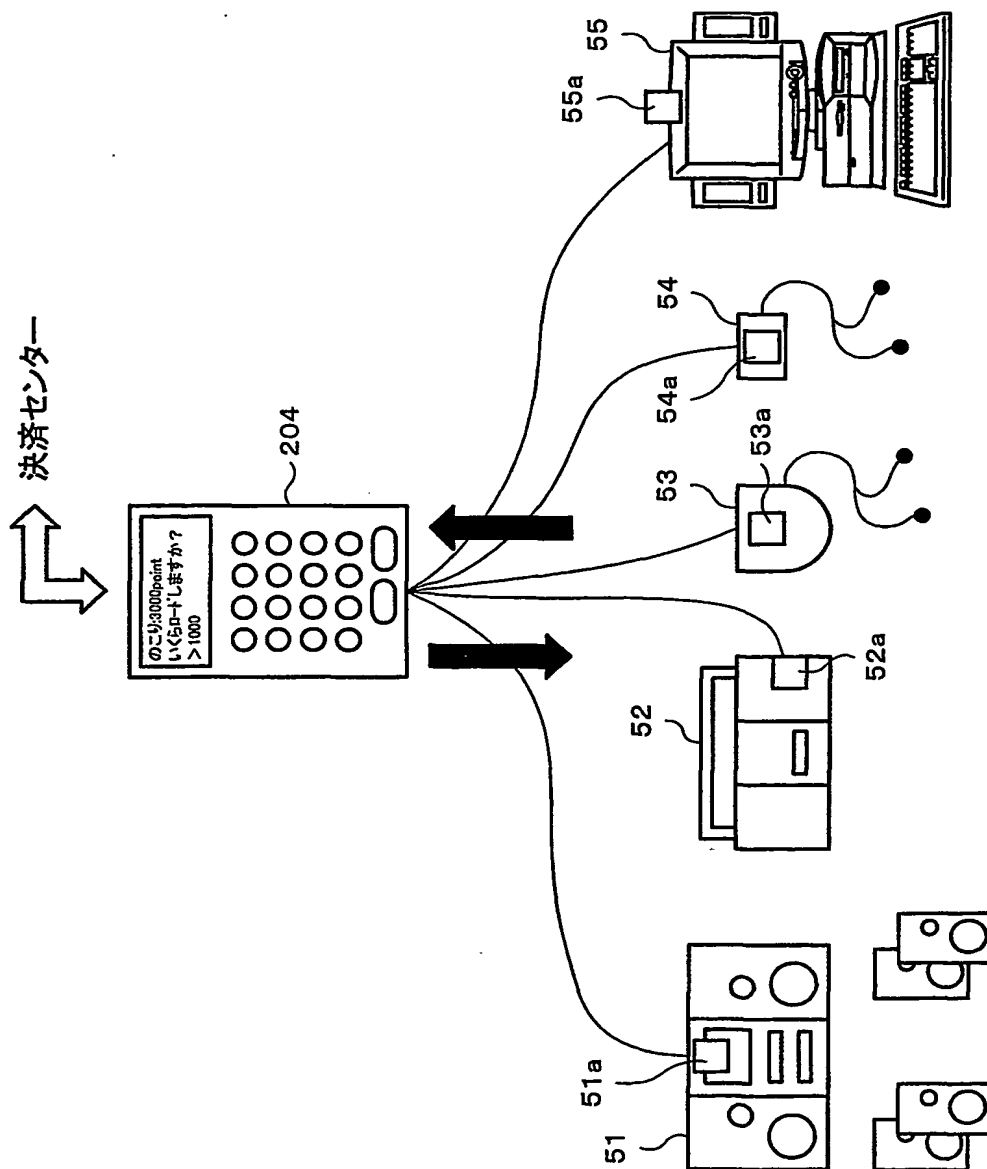
**THIS PAGE BLANK (USPTO)**

第2図



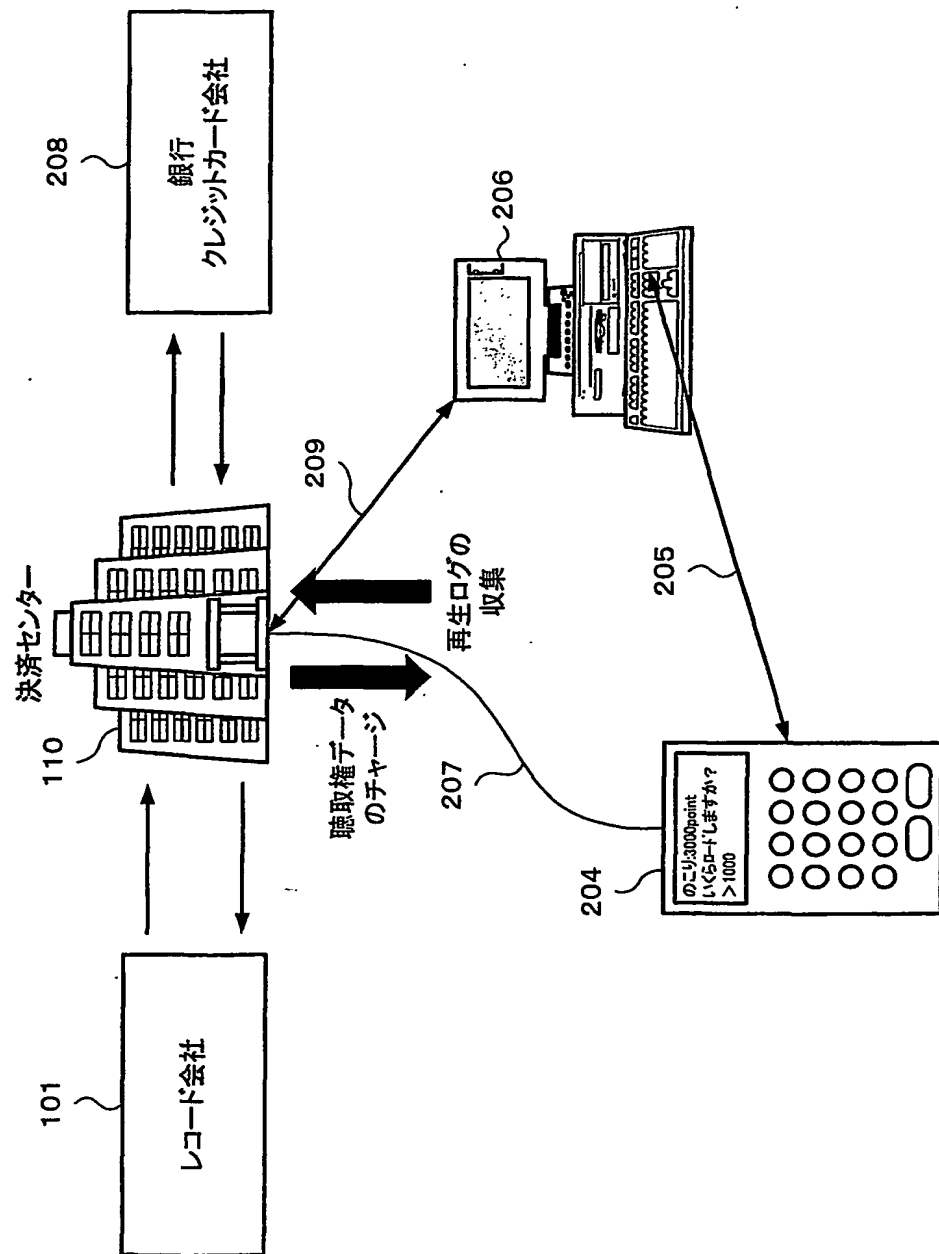
**THIS PAGE BLANK (USPTO)**

第3図



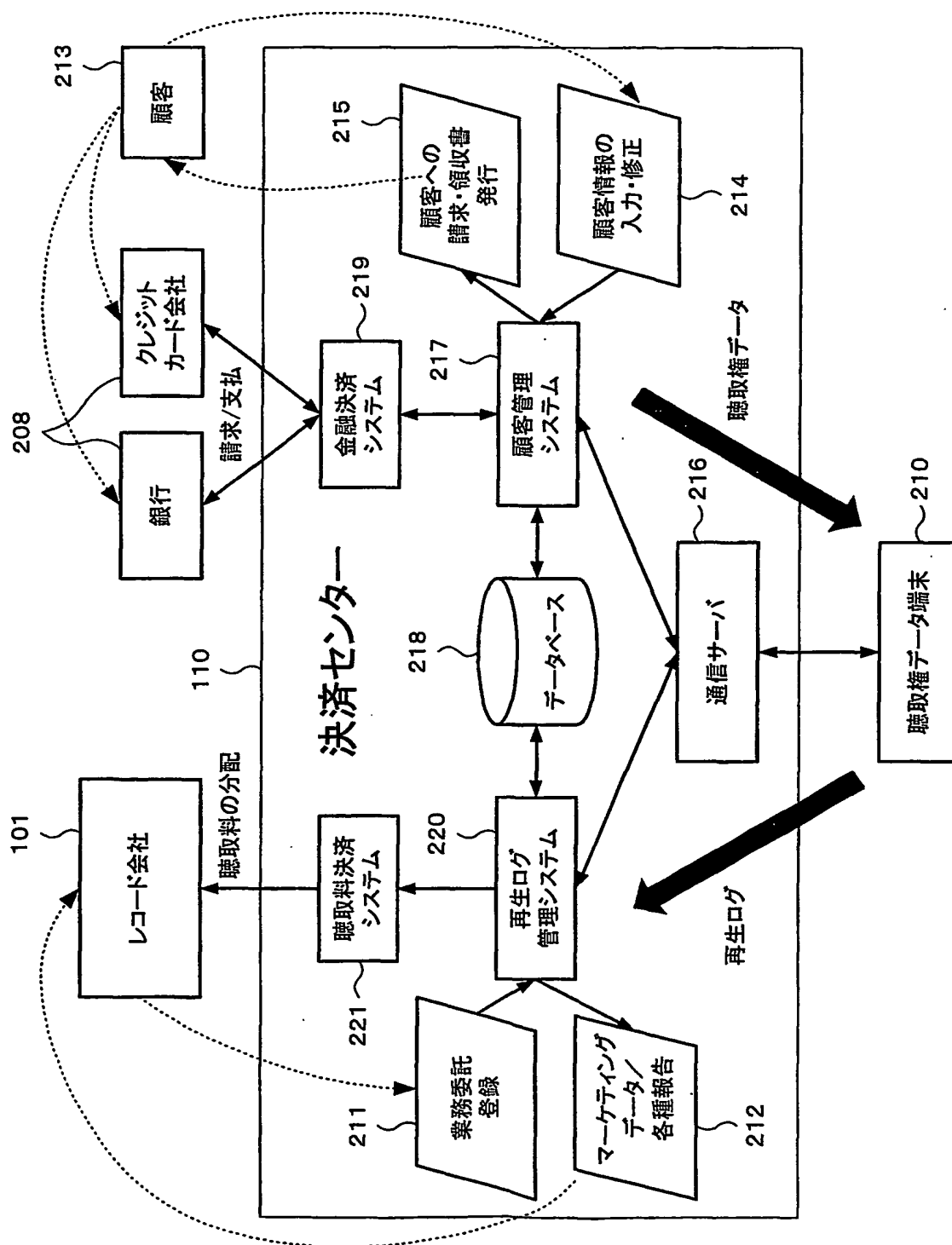
**THIS PAGE BLANK (USPTO)**

第4図



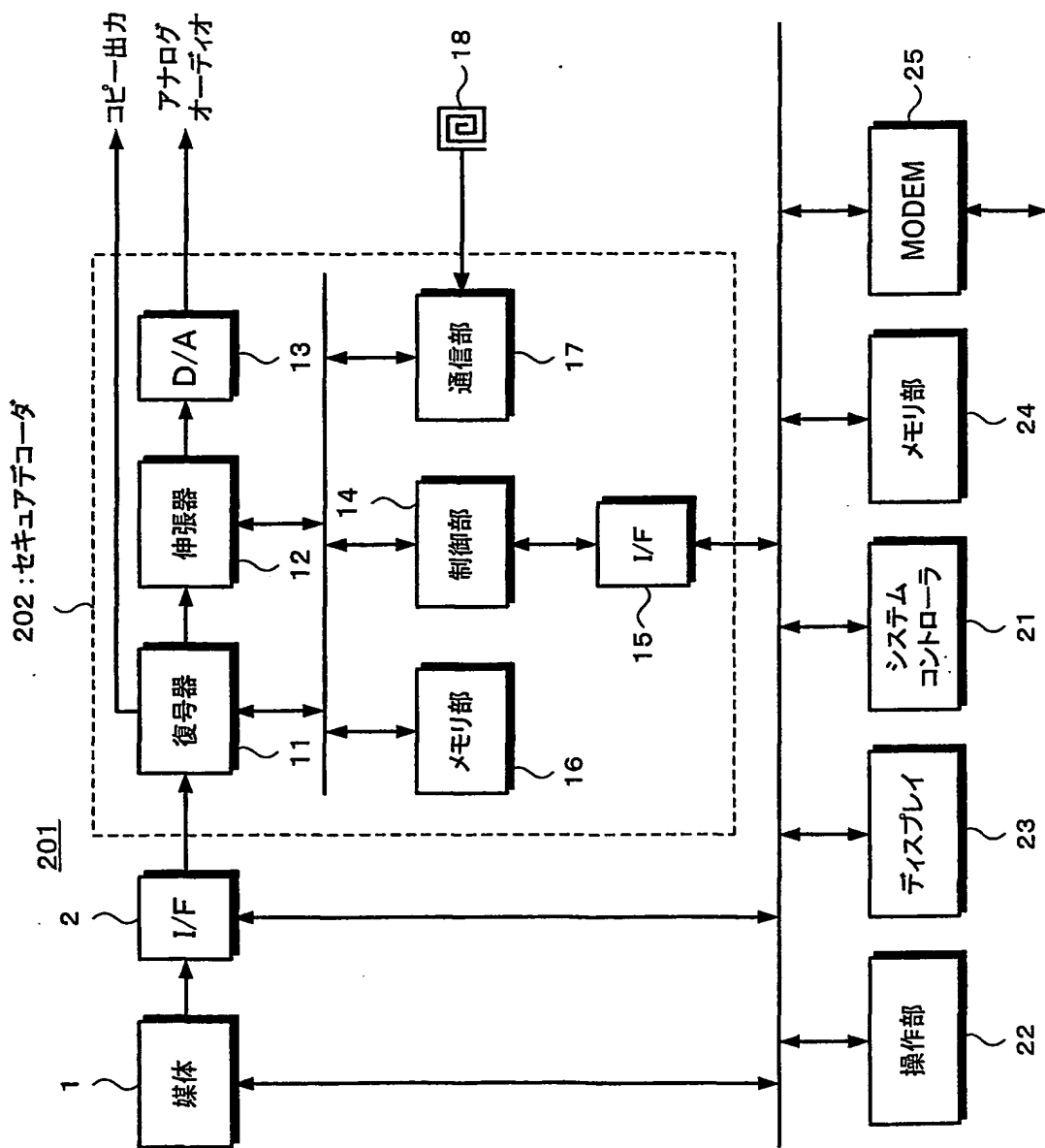
**THIS PAGE BLANK (USPTO)**

第5図



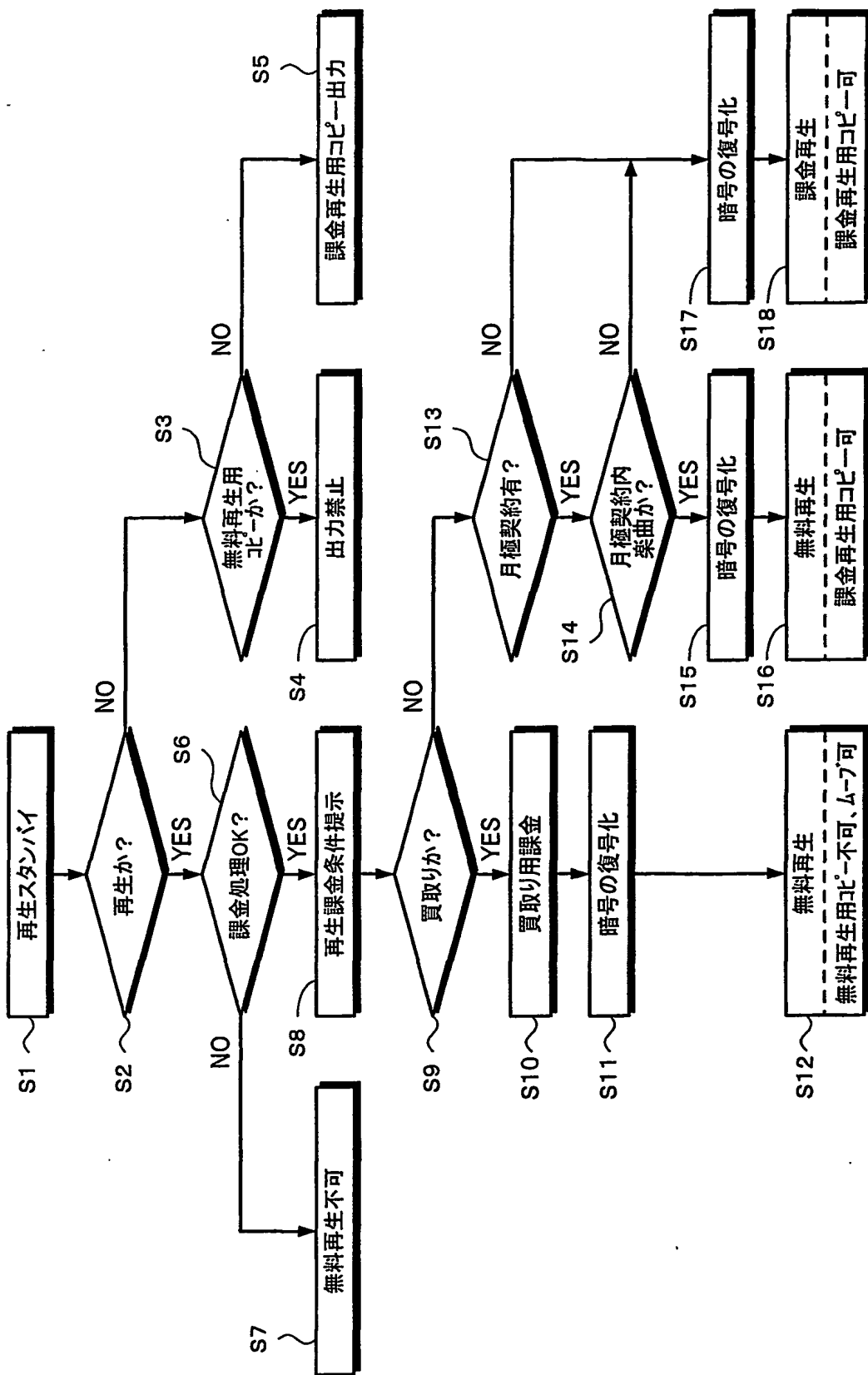
**THIS PAGE BLANK (USPTO)**

第6図



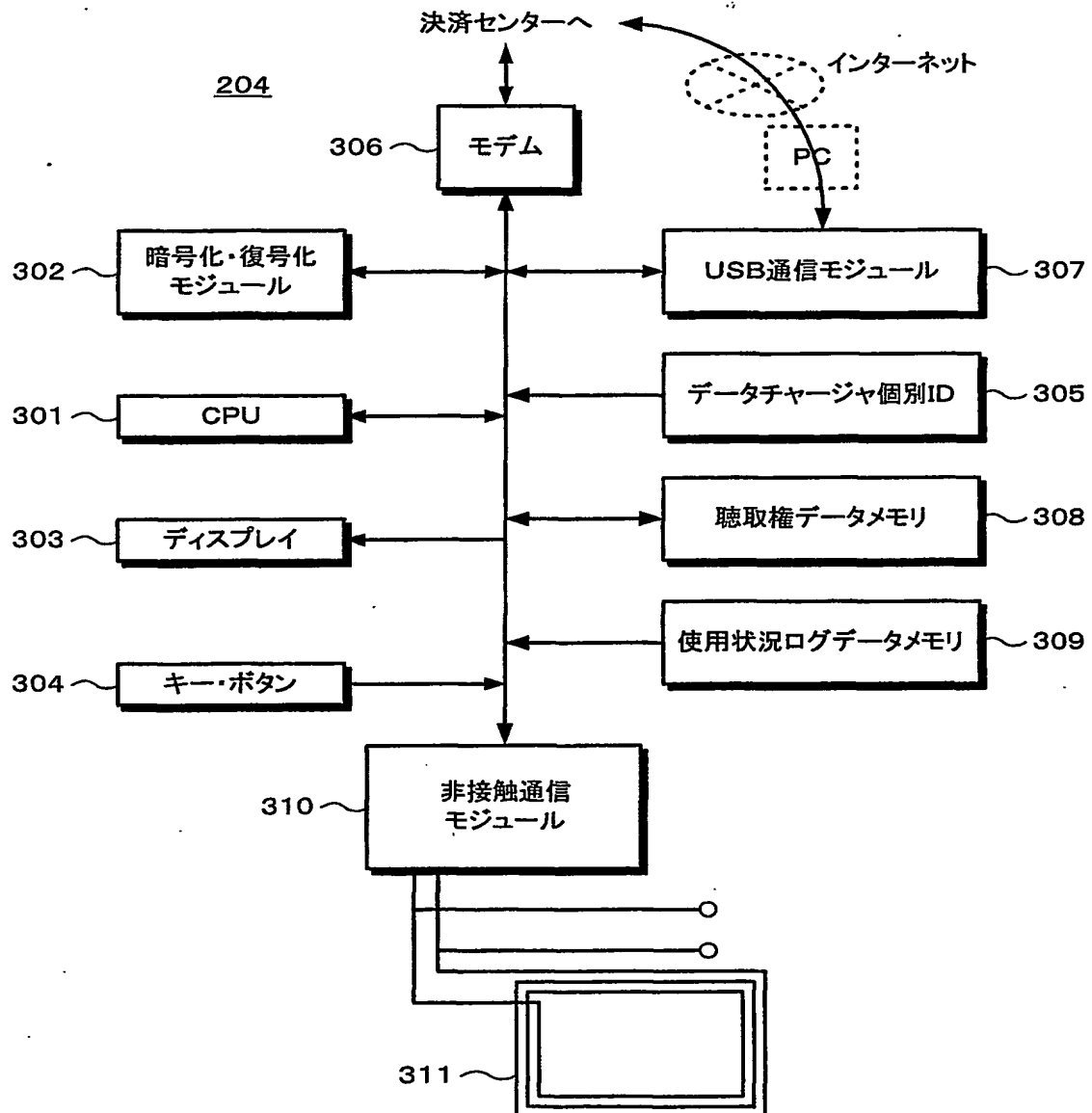
**THIS PAGE BLANK (USPTO)**

第7図



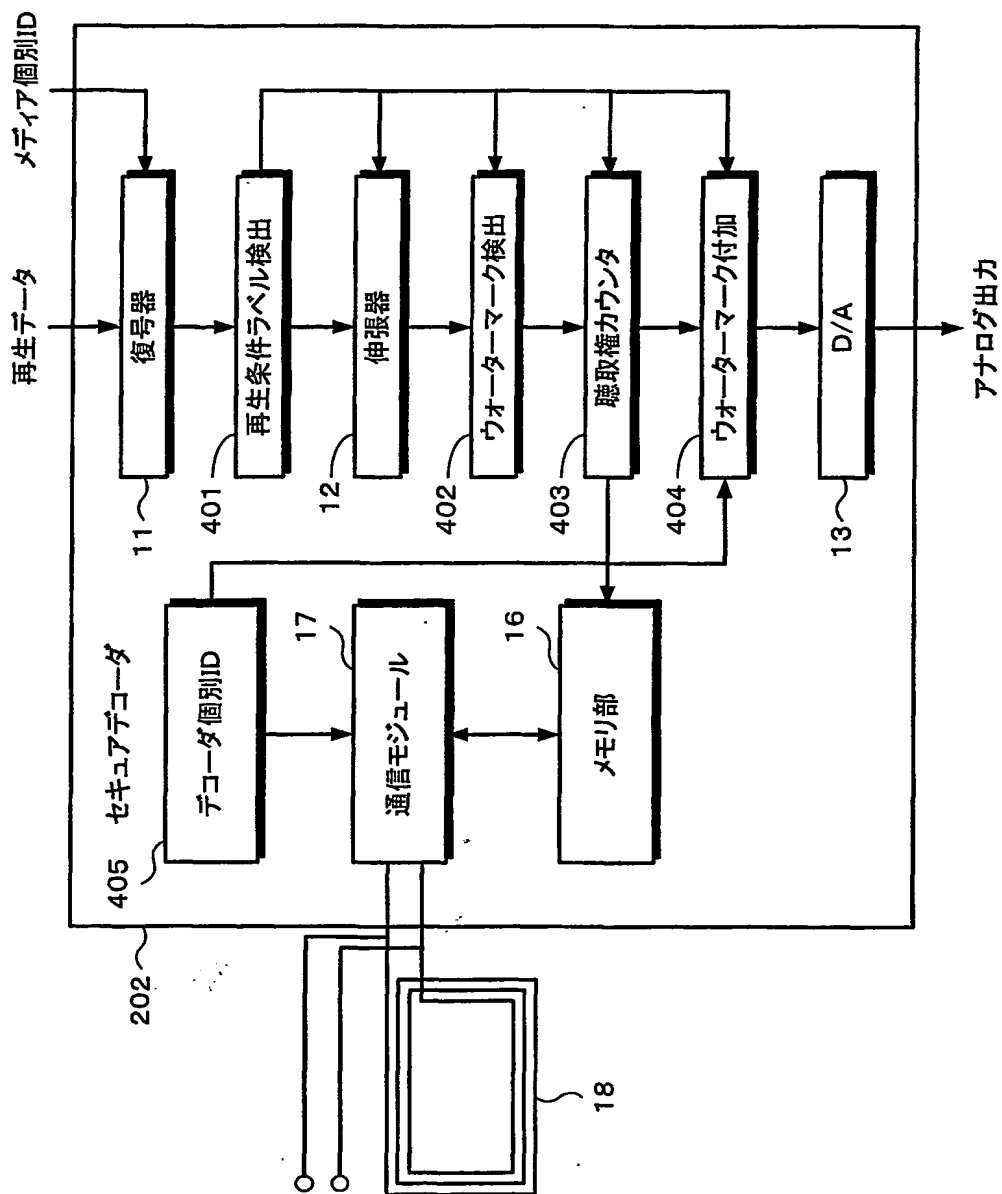
**THIS PAGE BLANK (USPTO)**

## 第8図



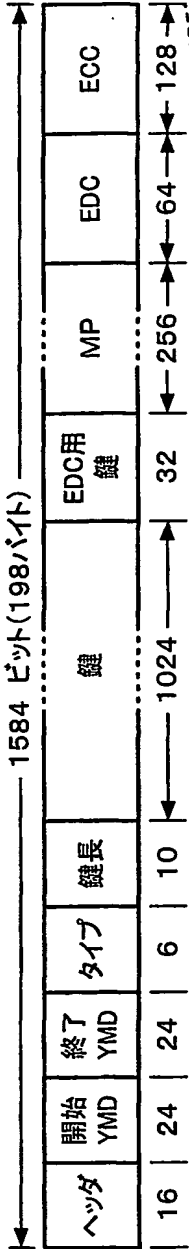
**THIS PAGE BLANK (USPTO)**

第9図

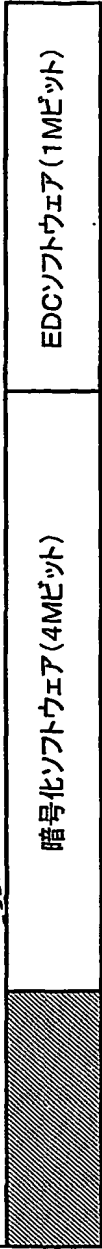


**THIS PAGE BLANK (USPTO)**

第10図A

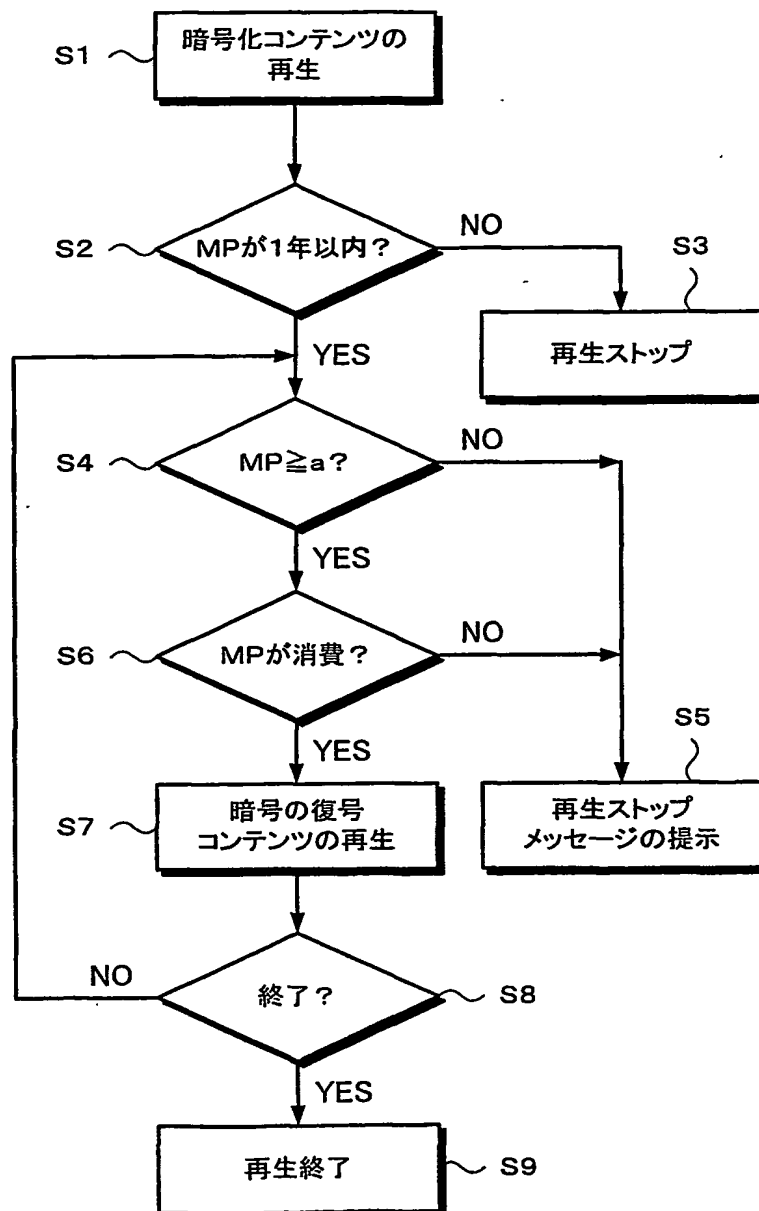


第10図B



**THIS PAGE BLANK (USPTO)**

## 第 1 1 図



**THIS PAGE BLANK (USPTO)**

## 符号の説明

- 1 コンテンツの格納された媒体
- 1 1 暗号化の復号器
- 1 2 圧縮符号化の伸張器
- 2 1 システムコントローラ
- 1 0 1 レコード会社
- 1 0 3 著作権管理機構
- 1 0 4 ユーザデバイス
- 1 0 9 聴取権データ
- 1 1 0 決済センター
- 2 0 1 プレーヤ
- 2 0 2 セキュアデコーダ
- 2 0 4 聴取権データチャージャ

**THIS PAGE BLANK (USPTO)**